



ILUSTRE MUNICIPALIDAD DE DALCAHUE

APRUEBA POLITICA GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

DECRETO ALCALDICIO N.º 1.407

DALCAHUE, 20 de mayo del 2024.-

VISTOS: Los numerales 04.01, 04.02, 05.01.01, 05.01.02 de la Norma Chilena ISO 27002 de 2009 referente a la Evaluación y tratamiento de riesgo y política de seguridad de la información; las facultades que me confieren los Artículos 4º, 5º d), 12º inciso cuarto, y 63º letras f) e i), todos de la Ley N° 18.695; el Decreto Alcaldicio N° 548 de fecha 07 de Marzo de 2022 que declara Alcalde de Dalcahue en relación a la sentencia firme y ejecutoriada del Tribunal Calificador de elecciones, Rol N° 1459-2021;

CONSIDERANDO: La necesidad de otorgar el adecuado respaldo jurídico administrativo a la definición de la estructura de la Municipalidad y a la asignación de funciones a las respectivas Unidades, con el fin de procurar su efectivo y coordinado ejercicio, tendiente a cumplir los objetivos que fija la ley, el Sr. Alcalde ha resultado dictar la siguiente POLITICA GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION.

POLÍTICA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

1 PROPÓSITO

La gestión de riesgos de seguridad de la información tiene como objetivo principal proteger la confidencialidad, integridad y disponibilidad de la información, así como salvaguardar los activos de información de la organización.

En este contexto, la Ilustre Municipalidad de Dalcahue establece las directrices para la gestión de riesgos vinculadas a la seguridad de la Información, para determinar la identificación, evaluación, tratamiento y monitoreo de los riesgos de seguridad de la información en la institución, determinando el marco de actuación aceptable para los niveles de riesgo inherentes, dentro del cual debe circunscribirse el desarrollo normal de esta, y las medidas apropiadas para la adecuada gestión riesgos.

2 ALCANCE O AMBITO DE APLICACIÓN

Esta política aplica a todos los activos de Información e incluso aquellos gestionados mediante contratos con terceros.

Aplica a todos los funcionarios (planta, contrata, reemplazos y suplencias), personal a honorarios y terceros (proveedores) que presten servicios para I. Municipalidad de Dalcahue.

Esta política se basa en lo definido en en la norma NCh-ISO 27002:2009 :

04.01 Evaluando el Riesgo de Seguridad .

04.02 Tratando los Riesgos de Seguridad.

Esta política abarca los siguientes controles definidos en la norma NCh-ISO 27002:2009 :

05.01.01 Documento de política de seguridad de la información.

05.01.02 Revisión de las políticas de seguridad de la información.

3 MATERIAS QUE ABORDA.

Establecer, formalizar y poner en práctica una metodología integral para la gestión del riesgo.

Definir y establecer el nivel aceptable de los riesgos.

Contar con la aprobación explícita de los planes de mitigación de los riesgos.

- Realizar evaluaciones periódicas de los procedimientos en uso para el control de los riesgos.
- Mantener informadas a las partes involucradas sobre el estado y el perfil de riesgos de seguridad de la información en el Municipio.

4 ROLES Y RESPONSABILIDADES

Directivos: responsables de generar las condiciones adecuadas para la ejecución y comunicación de la presente política, así como de establecer el alcance para su aplicación. Promover una cultura de gestión de riesgos de seguridad de la Información en toda la organización. Además, son responsable de asignar los recursos necesarios para implementar, mantener el proceso de gestión de riesgos y tratamiento.

Comité de Seguridad de la Información: El Comité de Seguridad de la Información (CSI) tiene la responsabilidad de supervisar y respaldar la gestión de riesgos de seguridad de la información del Municipio. Esto incluye la revisión regular de la efectividad de las políticas, directrices y procedimientos relacionados con la gestión de riesgos.

Encargado de Seguridad de la Información: Velar por el cumplimiento de la presente política y brindar asesoramiento en la identificación de las amenazas que pueden afectar a los activos de información y las vulnerabilidades que propician las mismas e informar al Comité de Seguridad de la Información sobre los resultados de la evaluación de los riesgos. Es responsable, en conjunto con los propietarios de los activos de información, por la definición de las acciones de tratamiento de los riesgos de seguridad de la información.

Los funcionarios Encargados de los activos de información: Quienes tengan a su cargo los activos tendrán que dar aplicación a la presente política e identificar, estimar y valorar los riesgos identificados. Es responsable, en conjunto con el responsable de seguridad de la información, por la definición de las acciones de tratamiento de los riesgos de seguridad de la información.

5 TERMINOLOGÍA

En este apartado se introducen los términos utilizados en la gestión de riesgos, su comprensión facilitará el resto de la lectura de la presente política.

Aceptación del riesgo: Decisión informada en favor de tomar un riesgo; la aceptación del riesgo puede tener lugar sin que exista tratamiento del riesgo o durante el proceso de tratamiento del riesgo.

Activos de información: toda información o recurso relacionado para la creación, almacenamiento, gestión o transmisión de dicha información. Podrán ser activos materiales (RRHH especializados, aparatos, equipos, redes, instalaciones, soportes y sistemas de almacenamiento) o intangibles (datos, aplicaciones, sistemas operativos, bases de datos, imagen, reputación, marcas de la organización).

Amenaza: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Análisis del riesgo: Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo. Para ello, tradicionalmente las metodologías proponen que se realice un inventario de activos, se determinen las amenazas, las probabilidades de que ocurran y los posibles impactos.

Apresiasi3n del riesgo: Proceso global que permite la identificaci3n del riesgo, el an3lisis del riesgo y su evaluaci3n.

Duefio del riesgo: Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo.

Impacto o consecuencia de la materializaci3n de una amenaza sobre un activo aprovechando una vulnerabilidad. El impacto se suele estimar en porcentaje de degradaci3n que afecta al valor del activo, el 100% ser3a la p3rdida total del activo.

Impacto: es la consecuencia de la materializaci3n de una amenaza sobre un activo. El costo para la instituci3n de un incidente de la escala que sea, que puede o no ser medido en t3rminos estrictamente financieros (ejem.: p3rdida de reputaci3n, implicaciones legales, entre otros).

Incidente: Evento inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes, equipos y sistemas de informaci3n.

Nivel del riesgo: Magnitud de un riesgo o combinaci3n de riesgos, expresados en t3rminos de la combinaci3n de consecuencias y de probabilidad.

Probabilidad: Es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento.)

Proceso de gesti3n de riesgo: Aplicaci3n sistem3tica de pol3ticas, procedimientos y pr3cticas de gesti3n a las actividades de comunicaci3n, consulta, establecimiento del contexto, e identificaci3n, an3lisis, evaluaci3n, tratamiento, seguimiento y revisi3n del riesgo. **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una p3rdida o dafio en un activo de informaci3n. Suele considerarse como una combinaci3n de la probabilidad de un evento y sus consecuencias

Riesgo de Ciberseguridad: Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes, equipos y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una de las amenazas antes mencionadas que produzca un impacto en términos de operatividad, o de integridad, confidencialidad o disponibilidad de datos.

Riesgo Inherente: Toda actividad, solo por el hecho de ser realizada, en sí tiene asociado un riesgo implícito (es decir, antes de aplicar controles). Es también llamado riesgo puro.

Riesgo residual: Riesgo remanente después del tratamiento del riesgo.

Tratamiento de los riesgos Para aquellos riesgos cuyo nivel está por encima del umbral deseado la institución debe decidir cuál es el mejor tratamiento que permita disminuirlos.

Vulnerabilidad o brecha informática: Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

6 DIRECTRICES DE LA POLÍTICA

6.1 Declaración Institucional

La I. Municipalidad de Dalcahue, declara su intención, promoción y aplicación de la gestión de riesgos de seguridad de la información de una forma adecuada y basada en marcos normativos ampliamente utilizados y consolidados a nivel global según la NCh-ISO 27002. Con el fin de gestionar los riesgos, sobre los activos vinculados a los procesos institucionales y de soporte, para el cumplimiento de los objetivos estratégicos, con foco en la ciberseguridad y asegurando la continuidad de los servicios críticos, para garantizar la confidencialidad, integridad y disponibilidad de la información.

6.2 Principios

Para los efectos de establecimiento de prácticas de gestión de riesgos, la presente política utilizará el enfoque proveído por la norma NCh-ISO 31.000:2018 sobre las directrices de un sistema de gestión de riesgos, puntualmente su apartado número 4, sobre los "Principios", señalados a continuación.

Principios Generales

Considerando la norma, que un riesgo es un "efecto de la incertidumbre sobre los objetivos", y la gestión de éste, las "actividades coordinadas para dirigir y controlar la organización con relación al riesgo", la presente política se orienta a establecer los principios detallados a continuación, y su aplicabilidad en el Municipio.

Integrada: La gestión de riesgos será parte integral de los activos de información que se encuentren asociados a los procesos tecnológicos, y de soporte a los servicios que entrega el Municipio.

Estructurada y exhaustivo: Se debe considerar un enfoque estructurado y exhaustivo hacia la gestión de riesgos, contribuyendo a resultados coherentes y comparables.

Adaptada: Los procesos de la gestión de riesgos se pueden adaptar, y son proporcionales a los contextos externos e internos del Municipio, en orientación a sus objetivos estratégicos.

Inclusiva: Considera la participación de cada parte interesada, con el objeto de conocer y considerar sus puntos de vista y recomendaciones, para promover consciencia y una gestión de riesgos informada.

Dinámica: Se debe considerar que los riesgos pueden cambiar en el tiempo, modificando sus evaluaciones e impactos respecto a los contextos del Municipio, por tal motivo, la gestión de riesgos debe detectar, anticipar y responder a cambios y eventos de una forma apropiada y oportuna.

Mejor información disponible: La información a considerar en la gestión de riesgos se debe basar en historia y actualización, así como también en su expectativa futura, la información a evaluar debe considerar además ser oportuna, clara y disponible.

Factores humanos y culturales: Se debe considerar el comportamiento humano junto con su cultura, las que influyen considerablemente en todos los aspectos de la gestión de riesgo.

Mejora continua: Se debe fomentar la mejora continua de la gestión de riesgos, considerando siempre el aprendizaje y experiencia.

7 MODELO DE ADMINISTRACIÓN DE RIESGOS

La I. Municipalidad de Dalcahue adopta un modelo con enfoque sistemático de gestión del riesgo de seguridad de la información para identificar las necesidades organizacionales en relación con los requisitos de seguridad de la información y para crear un sistema de gestión del riesgo de seguridad de la información (SGSI) eficaz.

La gestión del riesgo de seguridad de la información Municipal debe contribuir a lo siguiente:

7.1.1 Marco de gestión de riesgos

Se establece como marco de gestión de riesgos de la seguridad de la información del Municipio, el que define los procesos, las responsabilidades y los criterios para la identificación, evaluación, tratamiento y monitoreo de los riesgos. Las medidas de control necesarias para su mitigación, se monitorea su aplicación y se informa de sus resultados al nivel directivo de la institución.

El análisis de riesgos de seguridad de la información debe ser realizado de forma metódica implidiendo omisiones, improvisaciones o posibles criterios arbitrarios, bajo la adopción del siguiente marco.

El marco conceptual para la gestión de riesgos de la seguridad de la información es la norma ISO / IEC 27005: 2020, norma que aporta directrices para la gestión de riesgos de seguridad de la información.

7.1.2 Determinación del contexto

Se debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previos de su sistema de gestión de la seguridad de la información. Por tanto, se deberá determinar los condicionantes tanto internos como externos que definen el marco de trabajo.

A nivel interno se deberán tener en cuenta: la cultura, recursos, procesos y objetivos de la institución.

A nivel externo se consideran diferentes aspectos relativos al entorno social, económico, legislativo y de gobierno.

7.1.3 Determinación del Alcance y límites

Se debe definir el alcance y los límites de la gestión del riesgo de seguridad de la información de la I. Municipalidad de Dalcahue y el alcance del proceso de gestión del riesgo de seguridad de la información para garantizar que todos los activos relevantes se tomen en consideración en la evaluación del riesgo.

Adicionalmente, la organización debería proporcionar justificación para cada exclusión del alcance.

7.1.4 Identificación de Riesgos

La identificación de los riesgos de seguridad de la información debe ser realizada en conjunto entre las personas responsables de los activos en que se desenvuelve la Institución y el Encargado de Seguridad.

El modelo se basa en la asignación de una "Probabilidad de Ocurrencia" y una valorización de la "Consecuencia" o "Impacto" a cada uno de los eventos identificados, para así asignar prioridades y establecer las acciones de mitigación a implementar. El resultado de este análisis se resume en un Registro de Riesgos y en un Mapa de Riesgos Institucional.

El criterio para definir la probabilidad puede ser de tipo estadístico, basarse en la experiencia y/o conocimiento del dueño del activo y/o experto técnicos sobre la materia, o ser determinado mediante simulación u otras técnicas.

7.1.5 Valoración o apreciación de riesgos

Una vez definido el contexto se deben valorar los riesgos. Determinar los riesgos que van a ser controlados por medio de su identificación, análisis y evaluación. Todos aquellos riesgos que no sean identificados quedarán como riesgos ocultos o no controlados. Se deben realizar en esta fase las siguientes actividades:

Se debe llevar a cabo un proceso de identificación de riesgos de seguridad de la información en la organización. Este proceso incluirá la identificación de activos de información, amenazas potenciales, vulnerabilidades y posibles impactos, cuyo objetivo es búsqueda, reconocimiento y descripción de todos los posibles puntos de peligro tanto internos como externos; para cada uno de ellos se determinará su impacto y probabilidad.

Analizar el riesgo, se deberán calificar cada uno de los riesgos identificados tanto de forma cuantitativa (valorando su impacto) como cualitativa (importancia relativa) para priorizar los esfuerzos de forma no arbitraria. En esta actividad se debe comprender cómo se desarrollan los riesgos, estudiando sus causas y consecuencias, así como la evaluación de la eficacia de los diferentes medios de control implantados en la Institución. Se debe medir el nivel de riesgo, valorando las consecuencias y la probabilidad de cada riesgo.

Los riesgos identificados se deben evaluar utilizando una metodología adecuada, considerando la probabilidad de ocurrencia y el impacto potencial. La evaluación de riesgos permitirá determinar la prioridad de los riesgos y la necesidad de implementar medidas de mitigación. En esta fase se debe realizara la calificación del

análisis anterior incluyendo valoraciones en términos de estrategia de negocio que permitan establecer qué riesgos son aceptables y cuáles no.

7.1.6 Tratamiento de riesgos

Los riesgos evaluados se deben tratar utilizando una combinación de medidas de mitigación, transferencia, aceptación o evitación. Se deberán establecer planes de acción para abordar los riesgos de seguridad de la Información de manera efectiva.

Se deberán tomar decisiones frente a los diferentes riesgos existentes de acuerdo con la estrategia de la institución. Seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo.

De acuerdo con las siguientes opciones disponibles para el tratamiento del riesgo:

- Reducción del riesgo
- Aceptación del riesgo
- Evitación del riesgo
- Transferencia del riesgo

7.1.7 Comunicación de los riesgos de la seguridad de la información

La información acerca de los riesgos de los activos de información y tratamiento, se deben intercambiar y/o compartir entre quienes toman las decisiones y otras partes involucradas.

La coordinación entre las personas principales que toman las decisiones y las partes involucradas se puede lograr en el Comité de Seguridad de la Información (CSI) en el cual pueda tener lugar el debate acerca de los riesgos, su prioridad, el tratamiento adecuado y la aceptación.

7.1.8 Monitoreo y revisión

Se deben establecer el monitoreo y revisión periódica de los riesgos de seguridad de la Información. Esto permitirá identificar cambios en el entorno de riesgo y garantizar que las medidas de mitigación implementadas sean efectivas y adecuadas.

La organización deberá realizar el monitoreo continuo de los siguientes aspectos:

Activos nuevos que se han incluido en el alcance de la gestión del riesgo.

Modificaciones necesarias de los valores de los activos, por ejemplo, debido a cambios en los requisitos del negocio.

Nuevas amenazas que podrían estar activas tanto fuera como dentro de la organización y que no se han valorado.

Probabilidad de que nuevas vulnerabilidades o el incremento en las vulnerabilidades existentes permitan que las amenazas las exploten.

Vulnerabilidades identificadas para determinar aquellas que se exponen a nuevas amenazas o que vuelven a surgir.

El incremento en el impacto o las consecuencias de las amenazas evaluadas, las vulnerabilidades y los riesgos en conjunto que dan como resultado un nivel inaceptable de riesgo.

Incidentes de la seguridad de la información.

7.1.9 Mejora continua

Se debe fomentar la mejora continua del proceso de gestión de riesgos de seguridad de la Información. Esto incluye la revisión regular de la eficacia de las medidas de mitigación implementadas, oportunidades de mejora, la realización de ajustes según sea necesario y la implementación de acciones correctivas y preventivas.

La I. Municipalidad de Dalcahue debe implementar un proceso de gestión del riesgo de la seguridad de la Información y las actividades relacionadas sean las adecuadas. Todas las mejoras acordadas para el proceso o las acciones necesarias para mejorar la conformidad con el proceso se deberían notificar al Comité de Seguridad de la Información, para tener seguridad de que no se omite ni subestima ningún riesgo o elemento del riesgo, y que se toman las acciones necesarias y las decisiones para brindar una comprensión realista del riesgo y la capacidad para responder.

7.2 Consideraciones de Aplicabilidad de la Política de Gestión de Riesgos

Se considerarán actividades necesarias para la gestión de riesgos establecidas en la norma NCh-ISO/EIC 27001 :2020, y que son de aplicabilidad por la presente política, respecto a:

- Asegurar que el SGSI logre sus resultados previstos.**

- Prevenir o reducir los efectos no deseados.
- Lograr la mejora continua.
- Planificar las acciones para abordar riesgos y oportunidades.
- Integrar e implementar acciones en los procesos del SGSI, y evaluar su eficacia.
- Establecer y mantener la identificación, análisis y criterios de riesgo de seguridad de la información.
- Valorar los riesgos de seguridad de la información.
- Asegurar evaluaciones de riesgos de la seguridad de la información, para que produzcan resultados consistentes y válidos.
- Seleccionar las opciones apropiadas para el tratamiento de riesgos, considerando su evaluación.
- Determinar el conjunto de controles necesarios para implementar las opciones elegidas de tratamiento de riesgos de seguridad de la información.
- Elaborar una declaración de aplicabilidad de controles.
- Formular un plan de tratamiento de riesgos de seguridad de la información.

8 MECANISMO DE DIFUSIÓN.

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante el siguiente canal:

- Correo informativo institucional.

10 PERÍODO DE REVISIÓN.

La revisión del contenido de esta Política se efectuará a lo menos cada dos años por el Comité de Seguridad de la Información, o atendiendo necesidades de cambios para garantizar su idoneidad, adecuación y efectividad.

11 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

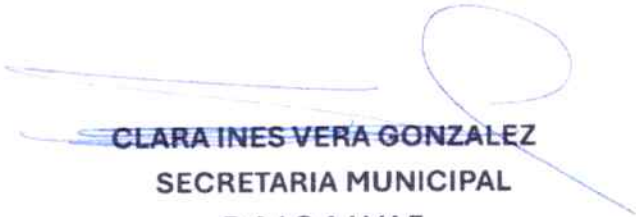
Frente a casos especiales, el comité de seguridad de la información, o el encargado de seguridad de la información, evaluará y podrá establecer condiciones puntuales de

excepción en el cumplimiento de las presentes directrices, siempre que no infrinja la legislación vigente. Toda excepción debe ser documentada y generar un proceso de revisión de la política, que determine si se deben agregar directrices en lo particular.

ANOTESE, COMUNIQUESE, PUBLIQUESE EN TRANSPARENCIA ACTIVA Y ARCHIVASE.



ALEX WALDEMAR GOMEZ AGUILAR
ALCALDE DE LA COMUNA DE DALCAHUE



CLARA INES VERA GONZALEZ
SECRETARIA MUNICIPAL
DALCAHUE

DISTRIBUCIÓN:

- Administración Municipal.
- Secretaría Municipal.
- Unidad de Control.
- Transparencia.

AWGA/CIVG/AEBB