República de Chile
Provincia de Linares
Dirección de Adquisiciones
Departamento de Informática

DECRETO EXENTO Nº: 741 /

PARRAL, 15 Febrero 2023

VISTOS:

1.- Las Facultades que me confiere la Ley N° 18.695/88, Ley Orgánica Constitucional de Municipalidades y sus posteriores modificaciones.
2.- La Sentencia definitiva de fecha 10 de junio del 2021 dictada por el Tribunal Electoral Regional del Maule.
3.- Acta de Proclamación de fecha 16 de junio del 2021 del Tribunal Electoral Regional del Maule.
4.- Juramento prestado en Sesión de instalación del Honorable Concejo Comunal de Parral celebrada el 28 de junio del 2021.
5.- Declaración de Asunción de funciones efectuada por el Decreto Afecto N° 1.282 del 29 de junio del 2021."
6.- El Decreto Exento Nº 2591 de fecha 06 de Julio del 2021, y Decreto Exento Nº 3360 de fecha 31 de Agosto del 2021, que corrige el considerando Nº 3 del Decreto Exento Nº 2591, que designa como Alcaldesa Subrogante, por orden de prelación a Doña Marie Michele Hiribarren Taricco, Directivo, Grado 6 E.M.S.
7.- El Decreto Exento N° 4569 de fecha 30 de Septiembre de 2011, que aprueba el Reglamento Interno sobre el Uso de Tecnologías de la Información de la Ilustre Municipalidad de Parral año 2021.-
8.- El Decreto Exento Nº 1702 de fecha 18 de abril de 2022, que aprueba la política de seguridad de la información para la Ilustre Municipalidad de Parral.

DECRETO:

1.- **ESTABLECESE**, el procedimiento de evaluación de riesgos a la seguridad de la información de la Ilustre Municipalidad de Parral.

PROCEDIMIENTO DE EVALUACIÓN DE RIESGOS A LA SEGURIDAD DE LA INFORMACIÓN DE LA ILUSTRE MUNICIPALIDAD DE PARRAL

Una evaluación de riesgos a la seguridad de la información es un procedimiento que permite a las instituciones identificar, analizar y aplicar controles de seguridad en el lugar de trabajo. Permite detectar vulnerabilidades y amenazas, evitando que se infiltren en la organización protegiendo los activos físicos e informativos de usuarios no autorizados.

Actualmente la ciberseguridad es fundamental para prevenir amenazas que podrían comprometer la seguridad de la información de la Ilustre Municipalidad de Parral, ayudan a prevenir peligros potenciales con capacidad e intención de explotar las vulnerabilidades existentes, protegen los datos sensibles de la Municipalidad como informacion personal o financiera contra ransomware o perdida de datos, cumplen con normas reglamentarias, clasifican los riesgos de cada activo y evalúan las operaciones de la institución.

OBJETIVO

Aplicar evaluaciones de riesgo a nivel institucional para evaluar mediante análisis y proporcionar recomendaciones a la Municipalidad para definir políticas y procedimientos para salvaguardar la informacion y permitir alcanzar un nivel de madurez digital óptimo para la Ilustre Municipalidad de Parral.

DEFINICIONES

- **Ordenador:** Maquina capaz de aceptar unos datos de entrada, efectuar en ellos operaciones lógicas y aritméticas, y proporcionar los datos resultantes a través de un medio de salida; todo ello sin la intervención de un operador humano y bajo el control de un programa de instrucciones previamente almacenado en el ordenador.
- **Hardware:** Conjunto de circuitos electrónicos, cables, dispositivos electromecánicos y otros elementos físicos que forman los ordenadores.
- **Software:** Conjunto de programas ejecutables por el ordenador.
- **Datos:** Es una información breve y concreta, proporcionada en un formato especifico y que puede ser procesada por un ordenador.
- **Información:** Es un conjunto de datos interrelacionados y ordenados según una estructura especifica, esta informacion puede almacenarse, procesarse y transmitirse electrónicamente, además de transformar su formato para su introducción y comprensión por un ser humano.
- **Internet:** Gran red internacional que permite, como todas las redes, compartir recursos. Es decir, mediante el ordenador, establecer una comunicación inmediata con cualquier parte del mundo para obtener informacion sobre un tema, conseguir un programa o un juego determinado para el ordenador. En definitiva: establecer vínculos comunicativos con millones de personas de todo el mundo, bien sea para fines académicos o de investigación o personales.
- **DNS:** Domain Name System. Sistema de nombres por dominios. Cada usuario tiene un nombre, una dirección única e irrepetible en la red. Al igual que cada teléfono tiene un número y no hay dos iguales, Internet asigna un nombre a cada ordenados. Este nombre no es aleatorio: corresponde a unas determinadas siglas relacionadas con la institución o red a la que está conectado.
- **Red:** Una red de comunicaciones es un conjunto de medios de transmisión y conmutación para el envió de informacion entre puntos separados geográficamente. Esta definición resulta extremadamente general y en la actualidad existen un gran numero implementaciones diferentes que responden a necesidades específicas, tales como redes de acceso de datos, troncales, inalámbricas, redes de voz, entre otros.
- **Proxy:** Un proxy se utiliza para filtrar las peticiones de paginas provenientes de los usuarios que se encuentran en su red local y con destino web situados en el exterior, es decir, internet.
- **Firewall:** Tiene como misión controlar los datos que entran y salen de la red, existen firewall por software y hardware.
- **Virus:** Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica mas relevante es que puede replicarse a si mismo y propagarse a otras computadoras. Infecta "entidades ejecutables": cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar. Se programa en lenguaje ensamblador y por lo tanto, requiere algunos conocimientos del funcionamiento interno de la computadora.
- **Antivirus:** Un antivirus es un programa cuya finalidad es prevenir y evitar la infección de virus, impidiendo también su propagación. Tiene capacidad de detectar y eliminar los virus y restaurar los archivos afectados por su infección.

- **Ransomware:** Software malicioso que al infectar un equipo da la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la informacion y datos almacenados.

METODOLOGIA

1. **Establecer y delimitar un marco de evaluación de riesgo**

   El proceso que evaluar debe ser objetivo, transparente y limitado, de tal forma que se obtengan resultados consistentes, aunque la tarea la desarrollen diferentes personas.

   Para establecer este proceso lo primero es identificar los requisitos, regulatorio o contractual, que le sean aplicables a la Municipalidad en el área de seguridad de la información.

   Se empleará la metodología de investigación basada en activos, la misma indicará los cambios correctos para el mejor control de los activos. Esta metodología evalúa y determina si los activos de la Municipalidad tienen vulnerabilidades por medio de la medición de la protección que tuvieses dichos activos, esto a su vez permite establecer varios controles que ayudan en gran medida a mejorar y disminuir los posibles riesgos.

   La evaluación por basada en activos esta compuesta de 4 etapas: **planificar**, se considera como el inicio de la evaluación y es aquí donde se dan los lineamientos a los que se piensa llegar. **Análisis**, en esta etapa se identifican y cuantifican todos los activos que se encuentran en la organización y a su vez se obtiene una estimación que se desee y se pueda controlar. **Gestión del riesgo**, en esta etapa se identifica las funciones y controles. **Selección**, en esta etapa seleccionan los controles.

2. **Identificación de los activos de la información**

   La evaluación de riesgos basada en activos es mas extensa en tiempo debido a la identificación de amenazas relevantes, pero entrega una visión completa en la que difícilmente un riesgo relevante escape.

   Se identifican los activos en software, hardware, redes de comunicaciones, instalaciones, servicios y personas.

   Para poder asignar un valor a los activos de la Municipalidad se han realizado las escalas de 3 valores con el fin que ofrezcan escalas de diferenciación de valores y se integra la planilla de levantamiento de activos.

	Valor	Clase	Descripción
Disponibilidad	1	Bajo	Los procesos de la Municipalidad no se ven afectados si esta informacion no se encuentra disponible.
	2	Mediano	Si la informacion no se encuentra disponible puede que afecte a los procesos que la utilizan. Sin embargo, existen métodos de contingencia para el desarrollo de operaciones o el proceso puede esperar hasta que se encuentre nuevamente la informacion disponible.
	3	Alto	Los procesos de la Municipalidad pueden llegar a tener un fatal efecto si esta informacion no se encuentra disponible en el momento que se le necesita.

Tabla Nº 1: “Disponibilidad de los activos de información”

	Valor	Clase	Descripción
Integridad	1	No requerida	Esta información es utilizada para consultas
	2	Requerida	Se requiere integridad en la informacion, pero si el contenido de esta llega a ser falsificado, las operaciones no se verían afectadas gravemente.
	3	Obligatoria	Puede causar un efecto fatal en las operaciones de la empresa si la integridad de esta informacion se perdiera.

Tabla Nº 2: "Integridad de los activos de información"

	Valor	Clase	Descripción
Confidencialidad	1	Acceso Publica	Informacion que puede ser revelada a terceras partes
	2	Acceso privado	Informacion que solo puede ser revelada a los funcionarios de la Municipalidad. Si el contenido fuera revelado a terceras partes, no hubiera mucho efecto en las operaciones de la Municipalidad.
	3	Restringido	Informacion que solo es revelada a partes especificas y departamentos de la organizacion. Si el contenido es revelado a personal no autorizado, puede haber un gran efecto en las operaciones de la Municipalidad.

Tabla Nº 3: "Confidencialidad de los activos de información"

Planilla de levantamiento de activos:

LEVANTAMIENTO DE ACTIVOS	
Nombre	
Departamento	

Aplicaciones / Servicios / Equipos Informáticos /Redes / Instalaciones / Personas			
Nº Inventario		Nombre	
Descripción			
Responsable			
Tipo			

Valoración	***Valor***	***Justificación***
Disponibilidad		
Integridad		
Confidencialidad		

FIRMA DE ACEPTACIÓN

3. Identificar puntos vulnerables y amenazas potenciales

Una vez identificados los activos de la información se procede a identificar los puntos vulnerables dentro de cada activo y las amenazas potenciales a estos. Esto permite tener un enfoque detallado en cada uno de los activos Municipales.

ORIGEN NATURAL	
Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta	
AMENAZA	***ACTIVOS***
Fuego	Equipos informáticos – Informacion - Instalaciones – Energía - Documentos
Daños por agua	Equipos informáticos – Información – Energía - Documentos
Desastre Natural	Equipos informáticos – Información – Instalaciones – Energía - Documentos
Afecta a:	**Disponibilidad del servicio**

Tabla Nº 4: "Amenazas de origen natural a los activos de información"

ORIGEN INDUSTRIAL	
Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada	
AMENAZA	***ACTIVOS***
Desastres industriales	Equipos informáticos – Información – Instalaciones – Energía - Documentos
Corte del suministro eléctrico	Equipos informáticos - Información
Condiciones inadecuadas de temperatura o humedad	Equipos informáticos - Información
Afecta a:	**Disponibilidad del servicio, confidencialidad de la información, integridad de los datos.**

Tabla Nº 5: "Amenazas de origen industrial a los activos de información"

ORIGEN NO INTENCIONADO	
Fallos no intencionales causados por las personas	
Amenaza	**Activos**
Errores de los usuarios	Datos – Claves – Servicios – Aplicaciones – Información
Difusión de software dañino	Aplicaciones
Fugas de información	Datos – Claves – Servicios – Aplicaciones – Información – Comunicaciones – Instalaciones - Personal
Vulnerabilidades de los programas (software)	Aplicaciones
Errores de mantenimiento actualización de programas	Aplicaciones
Errores de mantenimiento actualización de equipos (hardware)	Equipo informático
Caída del sistema por agotamiento de recursos	Equipo informático – Servicios – Redes
Restauración fallida de respaldos	Aplicaciones – Información
Indisponibilidad del personal	Personal
Afecta a:	**Disponibilidad del servicio, confidencialidad de la información, integridad de los datos.**

Tabla Nº 6: "Amenazas de origen no intencionado a los activos de información"

ORIGEN NO INTENCIONADO	
Fallos deliberados causados por las personas	
Amenaza	**Activos**
Suplantación de la identidad del usuario	Datos – Claves – Servicios – Aplicaciones – Redes
Uso no previsto	Servicios – Aplicaciones – Equipos informaticos – Redes – Información – Instalaciones
Modificación deliberada de la información	Servicios – Aplicaciones – Equipos informaticos – Redes – Información – Instalaciones
Divulgación de información	Servicios – Aplicaciones – Equipos informaticos – Redes – Información – Instalaciones
Manipulación de programas	Software
Manipulación de equipos	Equipos informaticos – información
Robo	Equipos informaticos
Ingeneria Social	Personal
Afecta a:	**Disponibilidad del servicio, confidencialidad de la información, integridad de los datos**

Tabla Nº 7: "Amenazas de origen no intencionado a los activos de información"

4. Determinar el impacto de las amenazas y vulnerabilidades

Finalizando la identificación de puntos vulnerables y amenazas potenciales se establece una lista de activos y una lista de riesgos que los amenazan.

En esta etapa se califican los riesgos en función de la probabilidad de ocurrencia, la degradación del activo y control de seguridad.

	Valor	Clase	Descripción
Degradación del activo	1	Bajo	Si ocurre la amenaza, el activo no se vería degradado gravemente.
	2	Medio	Si la amenaza ocurre, el activo se vería degradado de manera regular
	3	Alto	Si la amenaza ocurre, el activo se vería degradado gravemente

Tabla Nº 13: "Degradación del activo"

	Valor	Clase	Descripción
Probabilidad de ocurrencia	1	Bajo	Existe una baja probabilidad. La frecuencia de ocurrencia es una vez al año o menos.
	2	Medio	Existe una probabilidad moderada. La frecuencia de ocurrencia es una vez cada 6 meses o menos.
	3	Alto	Existe una alta probabilidad. La frecuencia de ocurrencia es una vez al mes o mas.

Tabla Nº 14: "Probabilidad de ocurrencia"

	Valor	Clase	Descripción
Control de seguridad	1	Alto	Controles establecidos y adecuados para combatir la amenaza.
	2	Medio	Control medio de seguridad.
	3	Bajo	Escasos o inexistentes controles de seguridad.

Tabla Nº 15: "Control de seguridad"

5. Gestión del riesgo

Posterior a la identificación del impacto de amenazas y vulnerabilidades y antes de considerar el tratamiento del riesgo, la Municipalidad debe decidir que medida tomar con cada riesgo. Se deben considerar las opciones para el tratamiento del riesgo:

- Evitar riesgo: cuando es posible y financieramente viable eliminar la causa raíz del problema
- Mitigar el riesgo: cuando es posible reducir la probabilidad de ocurrencia, el daño potencial de ambos.
- Transferir el riesgo: Subcontratando un proceso o tomando una empresa que se haga cargo del riesgo.
- Aceptar el riesgo: Cuando el costo de mitigarlo es muy alto y, por el contrario, es posible aprovechar alguna oportunidad aceptándolo.

La selección de controles debe ser sustentada por los resultados de la evaluación de riesgo. Las vulnerabilidades con las amenazas asociadas indican donde la protección pudiera ser requerida y que forma debe tener. Cuando se seleccionan los controles para la implementación, un numero de factores deben ser considerados:

- Uso de controles
- Transparencia del usuario
- Ayuda otorgada a los usuarios para desempeñar su función
- Relativa fuerza de controles
- Tipos de funciones desempeñadas

La valoración del riesgo se da una vez terminado el inventario de todos los activos de información, con su respectivo valor de confidencialidad, integridad y disponibilidad; la valoración de amenazas, en este caso, se desgloso en degradación de activo y probabilidad de ocurrencia, la cual se hace un promedio para sacar el valor total de la amenaza y por ultimo el valor de la vulnerabilidades.

Valoración de activo - A

Activo	Valor Asignado
Confidencialidad	A.1
Integridad	A.2
Disponibilidad	A.3

Valoración de amenaza - B

Amenaza		Valor
Degradación del activo	Probabilidad de ocurrencia	A=(A+O)/2
B.1	B.2	B

Valoración de vulnerabilidad - C

Vulnerabilidad	Valor
C - Vulnerabilidad	C

Una vez que todos estos valores están identificados se procede a calcular los riesgos por confidencialidad, integridad y disponibilidad de la siguiente manera:

1. Valor del riesgo por confidencialidad: R = A.1 * B * C
2. Valor del riesgo por integridad: R = A.2 * B * C
3. Valor del riesgo por disponibilidad: R = A.3* B * C

Una vez teniendo los valores de riesgo por disponibilidad, integridad y confidencialidad procedemos a ver si el activo se somete a evitar riesgo, mitigar el riesgo, transferir el riesgo o aceptar el riesgo.

6. Informe de evaluación de riesgo

Realizar un informe con toda la información trabajada en los 5 puntos anteriores, incluyendo hallazgos, planes de acción, plan de tratamiento de riesgos, entre otros. El propósito es generar un documento de respaldo de los objetivos, las acciones a realizar, la investigación, evaluación y análisis desarrollado.

ANOTESE, REFRENDESE, COMUNIQUESE Y CUMPLASE.

SECRETARÍA MUNICIPAL + ILUSTRE MUNICIPALIDAD DE PARRAL

SIGNIFLOW.COM

I. MUNICIPALIDAD DE PARRAL ALCALDE SUBROGANTE

SIGNIFLOW.COM

ALEJANDRA ROMAN CLAVIJO
SECRETARÍA MUNICIPAL

MICHELE HIRIBARREN TARICCO
ALCALDESA(S) DE PARRAL

MHT/ARC/EGH/EGP/JAH

DISTRIBUCIÓN

1.- Oficina de Partes
2.- Dirección Control (digital)
3.- Departamento de Informática (digital)
4.- COPIA DIGITAL (todos@parral.cl)

JULIO ABURTO HERNANDEZ	ERICA GAJARDO PEREZ
ENCARGADO DE T.I.	DIRECTORA ADQUISICIONES
SIGNIFLOW.COM	SIGNIFLOW.COM