Ministerio Secretaría General de la Presidencia

Gobierno de Chile

ORD. (DAG) N° 1801 /

ANT.: Solicitud de acceso a la información folio N° AF001T002187, de fecha 23 de noviembre de 2021.

MAT.: Ley N°20.285, sobre Acceso a la Información Pública.

SANTIAGO, 22 DIC 2021

A : [redacted]

[redacted]

DE : MÁXIMO PAVEZ CANTILLANA
SUBSECRETARIO GENERAL DE LA PRESIDENCIA

1. Esta Secretaría de Estado ha recibido su solicitud de acceso a la información pública citada en el antecedente, mediante la cual usted requiere lo siguiente:

"Solicitar información sobre normas y procedimientos de ciberseguridad. Esto es información para efectuar un proyecto con fines académicos, no tengo los contactos y por eso hago este tipo de solicitud por esta vía. Disculpe las molestias.

Necesito si me pueden responder estos tipos de preguntas.

• ¿Cómo está organizada la compañía? ¿Hay un CISO corporativo/múltiples? ¿No hay nada? ¿Oficial de riesgos? ¿CIO? ¿Otros roles?

• ¿Qué equipos existen en el área de seguridad?

• ¿Qué capacidades y tecnologías tiene la organización, cuáles no y cuáles fueron tercerizadas o delegadas?

• ¿Qué riesgos existen para este negocio en particular? (i.e. nation-state threats vs cibercrimen) ¿Qué podemos mencionar en general al respecto del riesgo?

• ¿Qué otros antecedentes en la industria son importantes conocer? (i.e. Colonial pipeline en energía).

• ¿Existe alguna regulación importante de conocer para esta industria?

• ¿Cuál es el activo digital más preciado de mi organización ("las joyas de la corona"). ¿Cómo pensamos en riesgos alrededor de este activo? ¿Cómo lo protegemos?

• ¿Cómo está la organización manejando su postura de seguridad? ¿Tenemos visibilidad? ¿Qué nivel organizacional tiene visibilidad de la postura?

• ¿Qué buenas prácticas de Seguridad en la Nube sigue la organización? ¿Cuáles podría adoptar y cuáles son las implicancias?

• ¿Cuál es el estado de madurez de la organización en términos de diseño de seguridad? ¿En qué fase suelen identificarse las amenazas? ¿Hay algún espacio de mejora?

• Considerar una Matriz de Riesgos ("mapa de calor"). Así no sea exhaustiva, podemos asumirla para efectos de presentar a un comité ejecutivo.

• ¿Qué tecnologías de seguridad puede identificar en su organización? ¿Cuáles representan una oportunidad? Considera un mapa de capacidades.

• ¿Qué tan preparada está la organización ante un Incidente de Seguridad? Considere todas las aristas, técnicas y no técnicas.

• ¿Cuáles serían las consecuencias de una disrupción operacional en su organización?

• ¿Su organización cuenta con un SOC? ¿Debería hacerlo?

• ¿El SOC deberá ser interno o externo?

• ¿Cómo gestiona su organización contraseñas y secretos? ¿Es seguro?

• ¿Qué tecnologías existen en el ámbito de la identidad de su organización?

• ¿Con qué organizaciones tiene mi organización una "relación de confianza"

para la autenticación o autorización?

• ¿Cuenta su organización con capacidades de auto-servicio? ¿Debería contar con ellas?

• ¿Su organización adopta la estrategia de Zero Trust? ¿Debería considerarla?""

2. Al respecto, el Ministerio Secretaría General de la Presidencia, cumple con responder cada una de sus preguntas:

- ¿Cómo está organizada la compañía? ¿Hay un CISO corporativo/múltiples? ¿No hay nada? ¿Oficial de riesgos? ¿CIO? ¿Otros roles?
  Respuesta: Existe un Oficial de Seguridad de la Información CISO
- ¿Qué equipos existen en el área de seguridad?
  Respuesta: Profesionales especializados en redes y seguridad, gestión de tecnologías, administración de infraestructura, ciberseguridad y desarrollo de software.
- ¿Qué capacidades y tecnologías tiene la organización, cuáles no y cuáles fueron tercerizadas o delegadas?
  Respuesta: Tiene todas las capacidades pada administrar su infraestructura tecnológica institucional con personal propio.
- ¿Su organización cuenta con un SOC? ¿Debería hacerlo?
  Respuesta: Sí

3. Respecto a los puntos 4, 7, 8, 9, 10, 11, 12, 13, 14, 17, 18, 19, 20 y 21, informamos que mediante la Resolución Exenta N°694, de 2021, de este origen, que Aprueba la Política General de Seguridad de la Información del Ministerio Secretaría General de la Presidencia, en el Punto III se refiere a las "Normas Generales de Seguridad de la Información", en su letra a), establece la Confidencialidad, integridad y disponibilidad de la información, indicando expresamente que "*la información constituye un activo de valor para la institución, razón por la cual es deber del personal resguardar el acceso por parte de personas no autorizadas y guardar reserva de la información y documentos que revisten el carácter de confidenciales*", por lo que no es posible entregar dicha información, debido al grado de sensibilidad y criticidad de su contenido para esta Cartera de Estado, resultando aplicable la causal de reserva contenida en el numeral 1 del artículo 21 de la Ley N°20.285.

4. Respecto a los puntos 5, 6 y 16, informamos que las preguntas no tienen relación con esta Secretaría de Estado.

Sin otro particular, saluda atentamente a Ud.,

REPUBLICA DE CHILE MINISTERIO SECRETARIA GENERAL DE LA PRESIDENCIA

MÁXIMO PAVEZ CANTILLANO
Subsecretario General de la Presidencia

FGR/ACC/CBJ/JRV/cps
DISTRIBUCIÓN:
1. [redacted]
2. MINSEGPRES (Gabinete Subsecretario).
3. MINSEGPRES (División Jurídica Legislativa).
4. MINSEGPRES (División de Administración General).
5. MINSEGPRES (Oficina de Partes).