



## ACTA DE ENTREGA

### SOLICITUD DE INFORMACIÓN PÚBLICA ROL C7827-20 CONSEJO PARA LA TRANSPARENCIA

#### I.- GENERALIDADES

1.- La decisión de amparo del Consejo para la Transparencia rol C7827-20, ha ordenado a la Subsecretaría de Salud Pública (...) "*copia de los correos electrónicos enviados y recibidos, desde sus cuentas institucionales, por la Subsecretaria de Salud Pública, Paula Daza; por el ex Ministro de Salud, Jaime Mañalich; por el actual Ministro de Salud, Enrique Paris; por el Director del DEIS, Carlos Sans; por Rafael Araos, del Departamento de Epidemiología; y por Johanna Acevedo, ex Jefa del Departamento de Epidemiología y actual Jefa de la Diplas, entre el 1 de marzo y el 12 de septiembre de 2020, ambas fechas inclusive*".

2.- El mismo fallo del Consejo establece que la entrega debe hacerse, debiendo tarjar, previamente, **los datos personales** de contexto y **datos sensibles** contenidos en la información a entregar, en los términos dispuestos en el considerando 16 de la presente decisión. Esto es "*por ejemplo, el número de cédula de identidad, domicilio particular, fecha de nacimiento, nacionalidad, estado civil, teléfono y correo electrónico particular, entre otros, así como también aquellos de carácter sensible, particularmente asociados al estado de salud de personas específicas identificables, en conformidad con lo dispuesto en los artículos 2º, letras f) y g), y 4º de la ley N° 19.628, sobre Protección de la Vida Privada, y en cumplimiento de la atribución otorgada a este Consejo por el artículo 33 letra m) de la Ley de Transparencia y el principio de divisibilidad consagrado en el artículo 11, letra e), del mismo cuerpo legal. En el mismo sentido se resolvieron los amparos Roles C706-18, C710-18 y C7206-20, referidos a correos electrónicos*".

3.- Que, en estas circunstancias, la Sra. Ministra de Salud encomendó evaluar la forma en la cual el Ministerio puede dar respuesta a la solicitud en los plazos establecidos, considerando que para el cabal cumplimiento de lo resuelto el Consejo para la Transparencia exige al Ministerio conciliar el principio de transparencia con el deber de resguardar los datos personales y sensibles contenidos en la información a entregar, sin perjuicio de que como se señalará, debe velarse por otros posibles datos que la misma ley N° 20.285 califica como sujeto a secreto o reserva.

4.- El Departamento de Tecnologías de la Información del Ministerio de Salud ha constado que la información solicitada por don Nicolás Sepúlveda Gambi equivale aproximadamente a [183 gigas], que corresponden aproximadamente a 72.000 correos electrónicos. Este volumen de información hace prácticamente imposible cumplir manualmente con el





mandato del Consejo para la Transparencia, siendo necesario diseñar soluciones tecnológicas.

4.- En este contexto, la Subsecretaría de Salud Pública hace presente diversas consideraciones para el proceso de entrega de la información solicitada, con una versión resumida de los puntos considerados en el proceso de tarjado de información sensible presente en los correos solicitados.

5.- Se previene que estas consideraciones fueron debidamente informadas al Consejo Para la Transparencia a través de una solicitud de aclaración **sin que dicho organismo manifestara reparo alguno** a las características de la solución informática diseñada por el ministerio.

## II.- CONSIDERACIONES GENERALES SOBRE LOS CORREOS ELECTRÓNICOS EXTRAIDOS

Las siguientes son algunas reglas preliminares definidas para el proceso de ocultamiento de información sensible:

- **IDENTIFICACIÓN DE RUTS:** se utilizó una función para detectar y tarjar todos los ruts presente en los textos. Por lo tanto, este proceso tarja ruts tanto de personas como de empresas. Puede que además el sistema tarje otros números que coincidan con el formato de ruts (números con puntos y guiones) como puede ser el caso de decretos u oficios.
- **IDENTIFICACIÓN DE EMAILS:** se utilizó una función para detectar todos los e-mails presentes en los textos, a fin de cautelar las casillas de correo que pueden ser dato personal. Con todo, se creó una lista de dominios públicos que no se tarjarán como @minsal.cl, gov.cl gob.cl. Como no se cuenta con todos los dominios públicos posibles, se identifican los principales a excluir pero es probable que algunos emails públicos queden tarjados en el procesamiento. Emails de universidades públicas se tarjan por la posibilidad de que pertenezcan a alumnos.
- **IDENTIFICACIÓN DE NOMBRES:** Para cada e-mail se tarjan todos los nombres propios de personas en el origen, destino, asunto y cuerpo. Si algún nombre aparece en el cuerpo del mensaje en mayúscula, se tarja. Si el nombre está en minúsculas se tarja solo si está antes o después de un apellido paterno que en su conjunto estén en el maestro de personas. Si en la sección de destinatarios aparece solo un nombre sin una dirección de e-mail, se tarja. Probablemente se tarjan nombres de funcionarios públicos al privilegiar la protección de datos de pacientes ante cualquier duda (alcance de nombres por ejemplo).
- **IDENTIFICACIÓN DE TELÉFONO:** se utiliza una función para detectar todos los números en formato de número de teléfono (por ejemplo que empiecen con +56). Por ende probablemente se tarjen cadenas de números que no correspondan necesariamente a teléfonos de personas. Se tarjan todos los números de teléfono encontrados, incluidos los de funcionarios públicos.



- **IDENTIFICACIÓN DE DIRECCIÓN:** para proteger las posibles direcciones de las personas presentes en los textos se tarjaron todos los números presentes en la colección de textos. De esta forma, puede que solo aparezca el nombre de una calle pero ningún número que permita identificar una dirección exacta. Bajo esta regla probablemente queden tarjadas cantidades de compra, fechas y todo otro tipo de número pequeño (menor a 7 dígitos) presente en los textos. Se tarjaron bajo el mismo sentido, comunas y provincias.
- **IDENTIFICACIÓN DE USUARIOS Y CONTRASEÑAS:** se utilizó una función para identificar la palabra "usuario:" y "contraseña:" en los textos y tarjar toda información referente al uso de cuentas en los sistemas de información utilizados por los funcionarios presentes en los textos.

Adicionalmente, se realizan las siguientes consideraciones:

1. Debe tenerse presente la posible existencia de correos duplicados en el universo de correos solicitados.
2. Se filtraron correos de tipo Calendario.
3. Los correos se encuentran en formato de "texto plano" incluso cuando los originales tienen formato con texto en html (enriquecido).
4. Únicamente se extrajo el asunto, fecha, emisor, receptor, con copia, con copia oculta, cuerpo del correo y nombre del archivo adjunto con un prefijo que identifica el origen del archivo. En el archivo de texto plano cada correo es separado del anterior por un tag: <eml> y una línea de inicio y fin para facilitar su lectura.

### **III.- MEDIDAS ADICIONALES PARA LA PROTECCIÓN DE DATOS DE FUNCIONARIOS PÚBLICOS Y PACIENTES**

1. Se eliminan todos los nombres en el cuerpo del correo, aunque sean funcionarios del Minsal, debido a que puede contener información de licencias médicas.
2. Se revisaron y tarjaron por completo correos que contengan las palabras: "Abuso", "Acoso", "Sumario" y "Sumaria".
3. Del mismo modo:
  - a) Nombres en mayúscula, correos, y nombres en minúscula conformados por dos palabras que en su conjunto son nombres en el maestro de datos.
  - b) Conceptos asociados a diagnósticos sensibles tales como "suicidio", "VIH", "SIDA", "inmunodeficiencia", filtrando los que hacen referencia a funcionarios o pacientes.
  - c) Usuarios de skype y otras redes sociales también deben ser eliminados.
  - d) Direcciones de correos extrañas a la Administración del Estado.

### **IV.- MEDIDAS DE PROTECCIÓN DE SISTEMAS DEL MINISTERIO**

1. Se revisaron y tarjaron por completo correos cuyo asunto contenga palabras asociadas a usuarios y contraseñas.




2. Se tarjaron en el documento la información de claves por medio de la búsqueda de palabras asociadas usuarios y contraseña.
3. Se tarjaron en el documento todas la URL que lleven a links o enlaces de descarga, debió a que pueden contener información sensible para los pacientes o para el ministerio.

El tarjado completo incluye todos los campos, es decir: asunto, fecha, emisor, receptor, con copia, con copia oculta, cuerpo del correo y nombre del archivo adjunto con un prefijo que identifica el origen del archivo.

#### V.- CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS SENSIBLES

El solicitante se compromete, conociendo los términos de la presente acta de entrega, a la no divulgación de los datos calificados como personales y sensibles por la ley N°19.628 sobre Protección de la Vida Privada, que encontrare en los archivos adjuntos o en el texto plano de los correos electrónicos que reciban

  
**MARÍA BEGONA YARZA SÁEZ**  
**MINISTRA DE SALUD**

  
**DR. CRISTÓBAL CUADRADO NAHUM**  
**SUBSECRETARIO DE SALUD PÚBLICA**

  
**NICOLÁS SEPÚLVEDA GAMBI**  
**SOLICITANTE**