**POLÍTICA DE USO CORREO ELECTRONICO INSTITUCIONAL**

**I.- DEFINICIONES ESTRATÉGICAS**

La empresa, a través de su [Comité de Riesgos y Seguridad de la Información], presenta en este documento la Política de Uso del Correo Electrónico Institucional, en consistencia con los principios rectores de la Política General de Seguridad de la Información.

**a.- Objetivos**

En específico, norma el uso del correo institucional, su respaldo y procesos de mantención de las cuentas de correo electrónico de la empresa, teniendo presente que las comunicaciones por esta vía son a título de representante de la empresa y no a título personal.

Con esta Política, la empresa, se compromete, a proteger sus activos de información, estableciendo una adecuada gestión del riesgo informático, asegurando el cumplimiento de los requisitos legales.

**b.- Alcance**

Esta política se aplica a todos los trabajadores y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la [Empresa XXX]. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea “presencial”, “a distancia”, “teletrabajo” u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el Presidente de la República.

Esta política gobierna la seguridad de la información de todos los procesos estratégicos de la [Empresa XXX], establecidos en el documento institucional denominado Definiciones Estratégicas o equivalente, cubriendo a toda la organización independiente de su ubicación geográfica en el país (Chile Continental, Chile Insular o la Antártica Chilena).

**c.- Roles y Responsabilidades**

Las responsabilidades se encuentran definidas en la política de la organización de la seguridad de la información.

**d.- Vigencia y Actualización**

La Política se considera vigente desde la fecha de su aprobación por parte de la autoridad, documento que será revisado y actualizado cada dos años o cuando el Comité de Riesgos y Seguridad de la Información lo determine, o toda vez que se produzca un cambio significativo que modifique el nivel de riesgo presente de la [Empresa XXX].

La Política deberá ser revisada por el Comité de Seguridad de la Información. No obstante, aquello, la [Unidad responsable de Ciberseguridad] promoverá la revisión permanente de esta Política y generará las propuestas de actualización que sean necesarias, con el objetivo de apoyar el ciclo de mejora continua del SGSI.

Entre los cambios que hacen necesaria la revisión de las políticas, se debe destacar:

* Cambios en las leyes o reglamentos que afecten a la [Empresa XXX].
* Incorporación o modificaciones relevantes de procesos críticos de la [Empresa XXX].
* Cambios significativos al soporte tecnológico.
* Modificaciones en la estructura de la organización.
* Cambios significativos en los niveles de riesgo a que se expone la información.
* Cambios relevantes en las Definiciones Estratégicas.
* Ajustes necesarios producto de Estados de Excepción Constitucional.
* Ajustes necesarios para proteger las infraestructuras críticas.

Las revisiones que se efectúen a la Política de General de Seguridad de la Información deben considerar tanto la actualidad de ella, como su eficacia, eficiencia y cumplimiento.

**e.- Revisión del cumplimiento**

El Comité de Riesgos y Seguridad de la Información, anualmente, asignará la responsabilidad de ejecutar un proceso formal de revisión del cumplimiento a cargo de una o varias unidades organizacionales, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

Además, este Comité determinará la metodología y los alcances que estime necesarios para cumplir los objetivos estratégicos de revisión y cumplimiento de las políticas y su mejora continua.

**f.- Control de documentos**

Los documentos requeridos por el Sistema de Gestión de la Seguridad de la Información (SGSI) deben protegerse y controlarse. Con este objetivo, las acciones necesarias a implementar son:

* Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
* Registrar los cambios o actualizaciones de los documentos una vez que son aprobados por el Comité de Riesgos y Seguridad, incorporando Tabla en Capitulo final en cada documento.
* Se deberá controlar el uso no intencionado de documentos obsoletos.
* En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo con los procedimientos aplicables a su clasificación.

**g.- Difusión**

El mecanismo de difusión de la Política será a través de la Intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el [Comité de Riesgos y Seguridad de la Información] estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

**II.- DIRECTRICES DE CIBERSEGURIDAD PARA EL CORREO ELECTRÓNICO**

El uso de la cuenta de correo electrónico de la empresa debe enmarcarse dentro del ámbito de su competencia y tener como finalidad el ejercicio de las funciones propias e inherentes para las cuales el personal ha sido contratado o se ha convenido su prestación de servicios.

**a.- Acerca del Correo electrónico institucional**

La [Unidad TIC] será la única responsable de la operación y provisión de él o los sistemas de correo electrónico de la empresa. Para lo anterior, empleará los dominios “@empresa.cl” o “@externos.empresa.cl” y procederá a la creación, bloqueo o eliminación de cuentas de correo electrónicos, sólo en el caso que sean visadas por el [Departamento de Desarrollo y Gestión de Personas].

En casos excepcionales, se podrá definir cuentas de correo electrónico asociadas a sistemas, para fines indispensables y absolutamente técnicos. Se podrán crear listas de correo, las cuales tienen el propósito de ser contacto corporativo asociada a equipo de personas responsables, las que deberán ser debidamente justificadas ante la [Unidad TIC].

Bajo ninguna consideración se podrán crear cuentas genéricas de correo o para grupos de usuarios, quienes, para sus comunicaciones, deberán emplear sus cuentas individuales. El personal no podrá contar con más de una cuenta de correo electrónico.

Se promoverá el correcto uso del correo electrónico de la empresa para lo cual a continuación se entregan lineamientos generales.

Se podrá utilizar servicios de correo electrónico en la nube, siempre que se informe a los usuarios de tal situación y se instruyan recomendaciones para el resguardo de los datos confidenciales o internos.

La [Unidad TIC] procurará tener acceso a toda la información que sea relevante para identificar anomalías en la utilización del correo electrónico o ataques dirigidos a este servicio, y dispondrá de herramientas para proteger la información sensible cuando deba enviarse por este medio.

El servicio de correo electrónico deberá contar con las configuraciones adecuadas para implementar, al menos, las siguientes características de seguridad: SPF, DKIM y DMARC.

**Identificación del remitente del correo electrónico institucional**

El correo electrónico debe contener la información suficiente para que el destinatario conozca con certeza la identidad del remitente y la empresa de procedencia.

La [Unidad TIC] procurará incorporar la firma digital[[1]](#footnote-1) en los correos electrónicos para garantizar la identidad del usuario emisor y el no-repudio de los correos electrónicos emitidos institucionalmente.

Complementariamente podrá evaluarse la utilización de la firma digital para certificar el sello de tiempo (*timestamp*) y el resguardo de la integridad y confidencialidad de las comunicaciones por este medio.

**Límite del almacenamiento de correo electrónico institucional**

La capacidad de cada cuenta de correo electrónico institucional podrá contener hasta [3 gigabytes] de información o la cantidad que la [Unidad TIC] determine de acuerdo con los recursos disponibles, y así mantener la estabilidad del programa de gestión de correos.

**Clientes y acceso de correo electrónico**

Los programas de correo electrónico a usar en la empresa deben ser los entregados por la [Unidad TIC], los cuales consideran un software para computador más los agentes y componentes de acceso remoto si el usuario posee un equipo portátil.

Los correos electrónicos podrán ser configurados en dispositivos móviles con conexión a Internet, tales como teléfonos celulares o Tablets. En estos casos se debe establecer que el dispositivo móvil tenga algún método de acceso o bloqueo mediante algún mecanismo de seguridad que el dispositivo posea. En el caso de pérdida o robo de estos dispositivos, el usuario deberá informar del hecho a la [Unidad TIC] con el fin de bloquear o cambiar la contraseña de correo electrónico.

La comunicación entre el dispositivo móvil y el servicio de correo electrónico debe ser encriptada.

**Envío de documentos por correo electrónico institucional**

El usuario no deberá enviar por correo electrónico documentos electrónicos que, individualmente o en conjunto, contengan más de [20 megabytes (MB)], o la cantidad que la [Unidad TIC] determine, salvo que el envío por otro medio o dispositivo electrónico, como CD, DVD, pendrive u otro, no sea posible. En todo caso, el usuario puede solicitar a la [Unidad TIC], la asesoría para determinar la mejor alternativa de compartir estos documentos.

El número de destinatarios de un correo está limitado para mitigar el riesgo de la posible utilización de cuentas institucionales para el envío de SPAM o correo basura. Si el uso de estos envíos masivos es frecuente o regular deberá privilegiarse la creación de grupos de correo.

Al enviar correo a una gran cantidad de destinarios y si éstos son desconocidos entre ellos o no requiera respuesta, debe considerar el envío en forma de Copia Oculta (CCO) del mensaje a todos aquellos, con el fin de evitar la divulgación de casillas de correo privadas que podrían ser usadas posteriormente para el envío de correos no deseados (SPAM). Si el grupo de destinatarios es permanente y con una recurrencia en su envío, puede solicitar la creación de un Grupo de Correo electrónico, que facilita el despacho de estos mensajes y la gestión de los destinatarios.

**Respaldo de correo electrónico institucional**

La [Unidad TIC] mantendrá copia actualizada del contenido de la casilla de correo de los usuarios hasta el tamaño del Límite del almacenamiento de correo electrónico establecido para atender casos de recuperación en caso de fallas de equipos y facilitar el acceso a éstos desde otros medios o dispositivos, cuyo tamaño está determinado por la disponibilidad de recursos.

La [Unidad TIC] podrá mantener un “archiving” o almacenamiento de respaldo “histórico” de correo, exclusivamente para las cuentas que sean solicitadas, casillas y alias institucionales vigentes asociadas a procesos y sistemas de gestión e información, considerando una ventana de tiempo de máxima de 2 años para revisiones o auditorías.

Cabe señalar que la necesidad de mantener respaldo de cuentas de correo y alias institucionales asociadas a procesos de gestión, no serán necesarias, en la medida que la gestión vaya incorporándose en el registro de auditoria de los Sistemas automatizados con medios informáticos. Con esto, la mantención de la información queda regulada por la política de gestión de activos de información.

**Exceso de correos electrónicos no descargados del servidor**

En caso de que el almacenamiento utilizado por correos electrónicos en el servidor exceda de la capacidad máxima por usuario establecida previamente por la [Unidad TIC], el personal autorizado o bien el sistema de manera automatizada advertirá al personal de dicha situación para que éste libere el espacio excedido.

**Uso de correo para fines no institucionales**

Las comunicaciones mediante correo electrónico, cuyos fines sean ajenos al ejercicio de las funciones laborales del personal o que no guarden relación con el ámbito de competencia de la empresa, no deberán efectuarse a través de una casilla de correo electrónico de la empresa.

En este sentido, si bien el uso de correos electrónicos no corporativos no está prohibido, no se encuentran soportados por la [Unidad TIC].

**No uso del servicio informático por un tiempo prolongado**

En el caso de personal con ausencia prolongada, más de seis meses, debido a permisos por maternidad, por enfermedad prolongada u otro motivo debidamente justificado, se podrá dejar el correo configurado con un mensaje de auto respuesta indicando la ausencia, más un destinatario alternativo del mensaje.

Sin perjuicio de lo anterior, el personal autorizado de la [Unidad TIC], previa consulta al [Departamento de Desarrollo y Gestión de Personas] cancelará o bloqueará la cuenta de correo según corresponda, que haya estado inactiva por más de 6 meses.

**Correos de cuenta para externos**

En caso de ser necesario, usuarios externos podrán contar con cuentas de correo debidamente señaladas y distintivas de las cuentas normales, para efectos de los servicios prestados a la empresa. Según las capacidades tecnológicas se establecerá una casilla que permita visualmente identificar el rol de externo, con la siguiente nomenclatura:

Formato: [Nombre.apellido]@[externos.empresa.cl]

**Direcciones electrónicas grupales**

Las direcciones electrónicas grupales o listas deberán ser solicitadas a la [Unidad TIC], debiendo en su nomenclatura plasmar funcionalidad que prestan. El formato para aplicar deberá estar normado por instructivos internos, y mientras estos no estén debidamente vigentes se utilizará el siguiente:

[Función].[área de la empresa]@empresa.cl

**b.- Seguridad y Auditorias de los Correos Electrónicos**

**Control de correo electrónico no deseado**

La [Unidad TIC] incorpora en el Sistema de Correo Electrónico, herramientas automatizadas para el control de SPAM o correo no deseado, y de manera general se podrán implementar alguno de estos criterios para su control:

* Listas blancas de IP o Servidores de organismos de confianza o con problemas de reconocimiento de correos válidos. Estos correos SI llegarán a la casilla del usuario final.
* Listas negras de IP reconocidas como emisoras de SPAM masivo se denegarán. Estos correos NO llegarán a la casilla del usuario final.
* Listas Grises de IP y usuarios tendientes a minimizar el SPAM robotizado mediante la obligación de solicitud de reenvío del correo cuando no se cumpla el criterio de la Lista gris.
* Filtro en base a ponderadores estadísticos (filtro bayesiano) considerando el contenido de cada correo electrónico. En este caso el correo SI llegará al buzón del usuario, pero con el “asunto de correo” modificado, mediante la adición de una etiqueta del tipo “[SPAM]”. En este caso se deja la decisión de eliminar el correo al usuario.
* Controles SPF / DKIM / DMARC
* Control DNSSEC
* Listas de reputación de IP’s.

**Protocolos de Seguridad**

La [Unidad TIC] procurará implementar los siguientes protocolos de seguridad para verificar la identidad de los remitentes en el sistema de correos electrónicos institucional ya que es una de las formas más efectivas de evitar que los envidadores de phishing y otros estafadores se hagan pasar por un remitente legítimo cuya identidad podrían suplantar utilizando el mismo nombre de dominio:

* SPF: El protocolo Sender Policy Framework o SPF, es un estándar de autenticación que vincula un nombre de dominio a una dirección de correo electrónico. Consiste en definir cuál es el remitente (o remitentes) autorizado para enviar emails con un dominio determinado. Este protocolo se utiliza para evitar el uso fraudulento de su nombre de dominio y evitar que terceros se hagan pasar por usted. Este protocolo es particularmente eficaz contra los ataques de phishing.
* DKIM: El protocolo DomainKeys Identified Mail o DKIM, es un protocolo criptográfico basado en el uso de claves públicas que se publican en su DNS. Este protocolo le permite firmar sus e-mails con su nombre de dominio, tal como lo haría al firmar una carta con su nombre. De esta forma, el destinatario de su e-mail podrá asegurarse de que la campaña que ha recibido ha sido escrita por usted y no ha sido alterada durante la transmisión. El objetivo del protocolo DKIM no es sólo demostrar que el nombre de dominio no ha sido usurpado, sino también que el mensaje no ha sido alterado durante la transmisión. Este protocolo es particularmente eficaz contra ataques de tipo "Man in the middle".
* DMARC: El protocolo Domain-based Message Authentication, Reporting and Conformance, o DMARC, es un estándar de autenticación que complementa a SPF y DKIM para combatir más eficazmente el phishing y otras prácticas de spamming. Permite a los propietarios de dominio indicar a los ISP (proveedores de servicios de Internet) y a los clientes de email qué hacer cuando un mensaje firmado de su dominio no está formalmente identificado por un estándar SPF o DKIM.

**Violación o Hackeo de la cuenta de correo electrónico institucional**

Un hackeo de cuenta de correo electrónico se refiere al hecho que la cuenta fue tomada por personas ajenas mediante el uso de ataques informático, robo de información o de algún computador o dispositivo móvil con dicha información.

En caso de que el usuario detectase acciones anormales en su cuenta de correo deberá notificar a la brevedad al equipo de seguridad de Informática, a fin de analizar la situación y aplicar los controles adecuados para proteger la información del usuario y la institución, cuando corresponda.

La [Unidad TIC], ante sospecha fundada de que la cuenta está siendo utilizada para fines potencialmente maliciosos, podrá bloquearla e informar al usuario de las actividades detectadas para que se apliquen las correcciones necesarias.

**Registros de eventos de correo (LOGS).**

El servidor de correo electrónico de la empresa guarda registro de información de las comunicaciones que circulan a través de él. Esto es básicamente información de fechas, emisor del correo, destinatario, entre otros datos técnicos, pero no registra ni almacena el contenido del correo en formato de LOGS.

Esta información técnica se utiliza para monitorear la operación del servidor y/o para detectar:

* Patrones que evidencien ataques realizados o en plena realización
* Posible origen de los ataques
* Accesos no autorizados
* Presencia de programas maliciosos en la red la empresa.
* Fallas en la operación del servidor o problemas en su configuración

**Garantías de entrega**

Aunque el porcentaje de entrega de los correos es muy elevado y llegan a su destino rápidamente, en ningún caso el servicio de correo electrónico garantiza la entrega de un mensaje.

En caso de requerir confirmación, el usuario deberá redactar sus correos con la opción de confirmación de lectura por parte de su destinatario, el cual podrá confirmar o no dicha recepción.

**Privacidad**

El Administrador del Servicio de Correo no podrá interceptar ni intervenir en modo alguno ningún mensaje, cuenta o casilla de correo de ningún usuario. Sin embargo, le asiste el deber de facilitar las acciones policiales y judiciales que así lo requieran.

En caso de requerimientos de acceso a cuentas de correo del personal por parte de las jefaturas, estas no serán autorizadas, salvo exista autorización explícita respaldada por la persona detrás de la casilla electrónica. En casos especiales, la situación deberá ser resuelta de manera conjunta por la [Unidad TIC] y la [Unidad Legal] por instrucciones del [directorio o Gerencia General] lo que procede realizar teniendo en consideración las protecciones constitucionales y de la dirección del trabajo a la vista.

**c.- Envío de correos electrónico con información confidencial.**

Se establece que el servicio de correo no cifra la información contenida en los correos, pudiendo ser eventualmente accesibles por terceros. De requerirse niveles adicionales de protección estos deberán ser solicitados a la [Unidad TIC], los que serán provistos en la medida de la disponibilidad de los recursos, las capacidades tecnológicas existentes y la pertinencia de la solicitud, bajo autorización expresa de la Jefatura de la Unidad.

Para la transmisión de información confidencial se deben incorporar técnicas avanzadas de cifrado y firmado de los correos electrónicos con el objetivo de proteger la información. Se debe coordinar con la [Unidad TIC] la asignación de recursos especiales para habilitar dichas funciones avanzadas.

El correo electrónico podrá contar con la capacidad de firma electrónica simple o avanzada de acuerdo con las necesidades específicas para al menos identificar formalmente al autor del correo electrónico, detección posterior de cualquier modificación, no repudio, entre otros atributos especificados en la Ley N° 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

Cabe destacar que un correo electrónico con firma electrónica avanzada podría llegar a considerarse un documento electrónico.

**d.- Estado de las cuentas de correo electrónico**

Se ha de tener en consideración que las cuentas de correo electrónico tendrán los siguientes estados:

* Activa: una cuenta de correo está activa cuando puede enviar y recibir mensajes con normalidad.
* Inactiva: Una cuenta de correo se considera inactiva cuando no se registra actividad (ingreso a la cuenta, envío de correo, etc.) por parte de un usuario.
* Bloqueada: Una cuenta de correo está bloqueada cuando no puede recibir ni enviar mensajes. Las causas de este bloqueo pueden ser, entre otras:
  + Por haberse llenado el buzón
  + Por haberse cumplido el plazo de inactividad establecido en la política.
  + Requerimiento de jefatura.
* Cancelada: Una cuenta de correo cancelada es una cuenta eliminada. Los mensajes dirigidos a una cuenta cancelada son rechazados devolviendo un mensaje de “cuenta de correo desconocida o inexistente”.

**e.- Restricciones en el uso del correo electrónico institucional**

* Los usuarios no deben crear, enviar, o retrasmitir mensajes de correo electrónico que puedan constituir acoso o que puedan contribuir a un ambiente de trabajo hostil.
* Los funcionarios no deben enviar o distribuir cualquier mensaje a través de los sistemas de la Institución, el cual pueda ser considerado difamatorio, acosador o explícitamente sexual o que pueda ofender a alguien con base en su raza, género, nacionalidad, orientación sexual, religión, política, discapacidad o FakeNews (desinformación).
* Los usuarios no deben utilizar los sistemas de la empresa para la transmisión de cualquier correo masivo no solicitado (SPAM, Phishing, MalSPAM).
* Los usuarios no deben emplear versiones digitalizadas de sus firmas manuscritas en los mensajes de correo electrónico.
* Los usuarios no deben utilizar las cuentas de correo oficiales para participar en grupos de discusión en Internet, Listas de Correo o cualquier otro foro público, a menos que su participación haya sido expresamente autorizada por la Autoridad a cargo de la Unidad a la que pertenece.
* Los usuarios tienen prohibido difundir software o contenidos que violen derechos de autor.

**f.- Creación, Eliminación o Cambios de Estado en las cuentas de correo**

Toda acción sobre el Estado de las Cuentas de correo, deberán ser requeridas por el [Departamento de Desarrollo y Gestión de Personas] y que corresponden a las definidas en el Punto “d.- Estado de las cuentas de correo electrónico”. En caso de estar asociadas a cuentas de sistemas, la [Unidad TIC] deberá realizar las consultas a la Unidad dueña del Sistema, de modo de garantizar la continuidad de las comunicaciones del Sistema con el personal y los clientes.

1. Ley N° 19.799 https://www.bcn.cl/leychile/navegar?idNorma=196640 [↑](#footnote-ref-1)