SIC-POL-01

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Propósito y alcance

El propósito de la "Política General de Seguridad de la Información", es declarar la estrategia de EOL Research con respecto al resguardo y protección de los activos de información corporativos. Esto se traduce en:

- Definir lineamientos o principios generales que sirven de medio para alcanzar los objetivos de un Sistema de Gestión de Seguridad de la Información, que incluye la Ciberseguridad.
- Establecer responsabilidades aplicables a los distintos niveles jerárquicos y a todo el personal vinculado a EOL Research.
- Fijar directrices de seguridad de la información que tengan un mayor grado de detalle, que apliquen a temas o sistemas específicos que sean de interés de la empresa.

2. Definiciones

Activo de Información

Aquello que tenga valor y es importante para EOL Research, sean documentos, sistemas o personas. Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la empresa. Se distinguen tres niveles:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.).
- Los equipos, sistemas e infraestructura que soportan o contienen esta información.
- Las personas que utilizan la información, y que tienen el conocimiento de los procesos de la empresa.

Colaborador

Toda persona que tenga un vínculo contractual de trabajo con EOL Research, sea éste indefinido, a plazo fijo o a honorarios.

Política

Directriz u orientación general expresada formalmente por la administración de EOL Research.

Norma

Disposición de carácter general que se desprende de las políticas, estableciendo obligaciones, restricciones, prohibiciones u otras conductas esperadas.

Procedimiento

Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles, en este caso, de Seguridad de la Información.

Riesgo

Es la posibilidad que ocurra un evento que afecte adversamente el logro de los objetivos de EOL Research. Se mide combinando las consecuencias del evento (impacto) y su probabilidad de ocurrencia.

Amenaza

Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o proceso.

Vulnerabilidad

Debilidad de un activo o grupo de activos que puede ser materializada por una o más amenazas.

Evento de Seguridad de la Información

Actividad o serie de actividades sospechosas que amerita ser analizada desde la perspectiva de la Seguridad de la Información.

Incidente de Seguridad de la Información

Evento o serie de eventos de Seguridad de la Información, no deseados o inesperados, que compromete la Seguridad de la Información y amenaza la operación del negocio.

Confidencialidad

Propiedad de la información que determina que sólo podrá ser accedida por personas, entidades o procesos debidamente autorizados.

Integridad

Propiedad de la información según la cual sólo puede ser modificada, agregada o eliminada por las personas o sistemas autorizados para cada proceso, de tal forma de salvaguardar la exactitud y completitud de los activos de información.

Disponibilidad

Propiedad de la información según la cual es accesible y utilizable oportunamente por las personas o sistemas o procesos autorizados, en el formato requerido para su procesamiento.

Modelo de Seguridad de la Información (MSI)

Es el conjunto de políticas y normas de Seguridad de la Información que definen y describen el diseño de los controles de seguridad de la información, basados en la normas ISO 27001, ISO 27002 e ISO 27032, que se aplican, o se aplicarán, en EOL Research.

3. Cláusulas de la política

3.1. De la información interna.

La información es un activo vital, por lo que su utilización, es decir, accesos, procesamiento y mantenimiento deberán ser consistentes con lo instruido en las políticas, normas, y procedimientos emitidos por EOL Research en cada ámbito en particular.

La información debe ser protegida, por sus custodios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información. A este conjunto de políticas y normas se le llamará también “Modelo de Seguridad de la Información”.

Toda información creada o procesada por EOL Research debe ser considerada como "interna", a menos que se determine expresamente lo contrario. EOL Research proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo con sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameritan.

3.2. De la información de los usuarios externos.

Si EOL Research procesa y mantiene información de usuarios externos que sean datos personales y/o sensibles de acuerdo con la normativa vigente, EOL Research se compromete a asegurar que esta información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna, de conformidad a lo establecido en la Ley N° 19.628, sobre protección a la vida privada, sin perjuicio de lo señalado en la ley N° 20.285.

En el caso de información de usuarios externos que se procese, mantenga y que no tenga las características anteriormente mencionadas, ésta podrá ser divulgada sin previa autorización.

Si se requiere compartir información de los usuarios externos de EOL Research con empresas externas, con motivo de externalizar servicios, a éstas se les exigirá un contrato, cláusula y/o convenio de confidencialidad y no divulgación previa a la entrega de la información.

3.3. De las auditorías.

Con el fin de velar por el correcto uso de los activos de información, EOL Research se reserva el derecho de auditar en cualquier momento el cumplimiento de las políticas y documentos vigentes que digan relación con el acceso y uso que los usuarios hacen de los activos de información. Las auditorías podrán ser realizadas internamente, a través un auditor interno, o por auditorías a cargo de organizaciones externas, cuando sea pertinente y requerido por el Comité de Seguridad de la Información.

3.4. De la gestión de la seguridad de la información.

La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por EOL Research. Este proceso de gestión deberá ser aplicado a los procesos de negocio críticos de EOL Research.

El cumplimiento de los objetivos del sistema de gestión de EOL Research se basará en la identificación de los activos de información involucrados en los procesos de negocio críticos, lo que implica al Encargado de Seguridad de la Información, junto a los responsables de los diferentes procesos y subprocesos de las actividades de EOL RESEARCH, realizar las siguientes acciones fundamentales:

- Identificar y clasificar los activos de información involucrados.
- Para cada activo de información, identificar un responsable.
- Analizar el riesgo al cual están expuestos.
- Difundir en forma planificada entre todo el personal de EOL Research el objetivo corporativo de la preservación de la información, sus características y las responsabilidades individuales para lograrlo, inserto esto, en planes de capacitación anual de EOL Research como actividades permanentes y en el proceso de inducción del nuevo personal.

3.5. Deberes del personal y de terceros.

Los deberes del personal y de terceros son:

- La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el servicio y autorizados por la jefatura directa, debiéndose aplicar criterios de buen uso en su utilización.
- Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.
- El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos que se establezcan en el manejo de incidentes.
- Se prohíbe la divulgación de información que esté considerada o clasificada como “reservada o confidencial”.

3.6. Organización de la seguridad.

Con el objetivo de garantizar el cumplimiento de la presente Política General de Seguridad de la Información y las políticas y normas específicas que sean definidas en el Modelo de Seguridad de la Información, EOL Research ha establecido una estructura organizacional de seguridad que contempla la definición de funciones específicas en el ámbito de seguridad, las cuales se encuentran señaladas en el documento específico "Política de Organización de la Seguridad de la Información".

3.7. Revisión de la Política.

La Política General de la Seguridad de la Información de EOL Research se revisará por lo menos una vez al año o ante cualquier cambio significativo de tecnología, personal o evento que amerite su reevaluación para asegurar continuidad, idoneidad, eficiencia y efectividad.

3.8. Difusión de la Política.

La gerencia de EOL Research considera fundamental integrar la seguridad de la información en la cultura organizacional, por lo cual desarrollará planes anuales de de difusión, capacitación y sensibilización en esta materia.

3.9. Otras políticas específicas de Seguridad de la Información

Se establecen y se consideran como parte de este marco normativo de Seguridad de la Información, políticas específicas de acuerdo con los catorce dominios definidos en la norma ISO 27002:2013, a saber:

- Políticas de Seguridad de la Información (el presente documento)
- Organización de la Seguridad de la Información
- Seguridad asociada a los Recursos Humanos
- Administración de Activos de Información
- Control de Acceso
- Criptografía
- Seguridad Física y Ambiental
- Seguridad de las Operaciones
- Seguridad en las Comunicaciones

- Adquisición, Desarrollo y Mantenimiento de Sistemas
- Relaciones con los Proveedores
- Gestión de Incidentes de Seguridad de la Información
- Seguridad de la Información en la Continuidad del Negocio
- Cumplimiento

3.10. Documentación de Seguridad de la Información.

La documentación de Seguridad de la Información de EOL Research es la siguiente:

- Modelo de Seguridad de la Información, compuesto por Políticas y Normas, que definen el diseño de los controles de seguridad de la información que se implementarán en la organización.
- Procedimientos, que describen las actividades y tareas relacionadas con los controles de seguridad implementados.

3.11. Documentación de referencia.

Se considerará como documentación de referencia para la presente política, toda la normativa vigente en Chile a esta fecha, a decir:

- Decreto Supremo No. 83 de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Ley N° 17.336, sobre Propiedad Intelectual.
- Ley N° 19.223 que tipifica figuras penales relativas a la informática.
- Ley N° 19.628, sobre protección a la vida privada.
- Ley N° 20.285, sobre acceso a la información pública.
- Ley N° 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Norma NCh- ISO 27001:2013.
- Norma NCh- ISO 27002:2013.
- Norma NCh- ISO 27032:2012.

HISTORIAL DE CAMBIOS

Fecha	*Descripción del cambio*
10-03-2021	Elaboración del documento original