POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Registro de Modificaciones / Autorizaciones				
Nº	**Fecha**	**Nombre/Dpto**	**Descripción**	**Firma**
0	04/10/2016	Hernán Gianini / Consultor	Emisión	
1	10/03/2022	Daniel Vénere / Consultor	Actualización de directrices generales	
2	08/01/2023	Francisco Leal / Consultor	Actualización a la norma PCI DSS	
3	17/03/2023	Francisco Leal / Consultor	Actualización a la normativa CMF	
3	06/03/2023	Javier González / Gerente General	Aprobación de la Política	JAVIER IGNACIO GONZALEZ FULLE Firmado digitalmente por JAVIER IGNACIO GONZALEZ FULLE Fecha: 2024.04.02 17:54:43 -03'00'
4	26/01/2024	Francisco Leal /CISO – Encargado de Riesgos, Cumplimiento y Prevención de delitos	Revisión del contenido	
4	06/02/2024	Javier González/Gerente General	Revisión del contenido	JAVIER IGNACIO GONZALEZ FULLE Firmado digitalmente por JAVIER IGNACIO GONZALEZ FULLE Fecha: 2024.04.02 17:54:59 -03'00'
4	06/02/2024	María Suarez/Gerente BPO	Revisión del contenido	
4	29/02/2024	Macarena Topali y Nicolás Jiménez/ Abogados	Revisión del contenido	
4	04/03/2024	Javier González/ Gerente General	Aprobación de la Política	JAVIER IGNACIO GONZALEZ FULLE Firmado digitalmente por JAVIER IGNACIO GONZALEZ FULLE Fecha: 2024.04.02 17:55:24 -03'00'

(*) La presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

CONTENIDO

OBJETIVO DEL DOCUMENTO

La presente política, tiene por objetivo establecer las directrices generales de seguridad de la información y ciberseguridad, que deben cumplir todos los colaboradores y prestadores de servicios de Proyectum, para:

- Mantener los activos de información:
  - Disponibles : Que permitan ser utilizados en el momento que sean requeridos.
  - Íntegros : Que solo sean modificados por personas autorizadas.
  - Confidenciales : Que solo sean conocidos por personas autorizadas.

- Prevenir que los colaboradores y/o prestadores de servicios, cometan los delitos informáticos indicados en la Ley N° 21.459 "Ley de Delitos Informáticos", esto implica y sin que la enumeración sea taxativa:

  - Ataque a la integridad de los sistemas informáticos de Proyectum, o de cualquier cliente de Proyectum.
  - Acceso ilícito a la información de Proyectum, o de cualquier cliente de Proyectum.
  - Interceptación ilícita, es decir, que intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, ya sea de Proyectum o de cualquier cliente de Proyectum.
  - Ataque a la integridad de los datos informáticos, ya sea de Proyectum, o de cualquier cliente de Proyectum.
  - Falsificación de información, ya sea para Proyectum, o cualquier cliente de Proyectum.
  - Receptación de datos informáticos, esto es el que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de conductas previamente indicadas, ya sea de Proyectum, o de cualquier cliente de Proyectum.
  - Cualquier fraude informático, esto quiere decir, que obtenga un beneficio económico causando perjuicio a otro, debido a la

manipulación de un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, ya sea de Proyectum, o de cualquier cliente de Proyectum.

- Abuso de dispositivos.

Cualquier otra conducta que implique una vulneración a la Ley N°21.459.

- Proteger los datos personales de nuestros clientes, colaboradores y/o proveedores de acuerdo con lo establecido en la Ley N° 19.628 "Protección de datos personales".

- Proteger los datos confidenciales de autenticación y autorización de los tarjetahabientes. Y dar cumplimiento a la norma PCI DSS.

- Cumplir con las normativas exigidas por la Comisión del Mercado Financiero (CMF) en materia de seguridad de la información y ciberseguridad.

ALCANCE DEL DOCUMENTO

La presente política es revisada anualmente y actualizada en su contenido, asegurando que el modelo de ciberdefensa sea cumplido obligatoriamente por todos los colaboradores y prestadores de servicios que acceden a los activos de información de Proyectum y sus clientes.

Las excepciones a la presente política aumentan los riesgos de ciberataques a la empresa y los activos de nuestros clientes, por lo tanto, deben ser justificadas y autorizadas por el Gerente General.

El alcance específico de la Política de Seguridad de la Información y Ciberseguridad se encuentra en:

Política de uso de tecnologías críticas

Política de gestión de continuidad de negocios

Política de riesgo operacional

Procedimiento de altas, bajas y modificaciones de accesos a los sistemas

Procedimiento de gestión y respuestas a incidentes de seguridad

Procedimiento de gestión de antivirus

Procedimiento de alta, baja y modificación de computadoras

Procedimiento de concientización de colaboradores

Procedimiento de monitoreo y gestión de vulnerabilidades

Procedimiento de gestión de proveedores

Reglamento de Orden, Higiene y Seguridad

Anexos de contratos con colaboradores

Anexos de contratos con prestadores de servicios

DEFINICIONES

Seguridad de la Información	:	La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.
Ciberseguridad	:	La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos
Ciberdefensa	:	Es el uso de medidas técnicas, administrativas y legales para proteger a una organización de amenazas informáticas.
Ciberataques	:	Un ciberataque o ataque informático es cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático.
PCI DSS	:	Es un estándar reconocido a nivel mundial para garantizar la seguridad de los datos de las tarjetas de pago y evitar filtraciones de seguridad.
Hacking	:	El hacking se puede definir como "la búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes.
Activos de Información	:	Son cualquier tipo de recurso que contenga información valiosa para una organización. Estos incluyen datos, documentos, correos electrónicos, software, sistemas, redes, dispositivos y bases de datos.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Se reconoce a la Gestión de Seguridad de la Información como un proceso crítico que debe involucrar a todos los niveles de la empresa, debiendo todas y cada una de las personas que la integran, comprender y asumir las responsabilidades respecto a proteger la información.

Toda la información, al igual que los riesgos a los que está expuesta deberán poseer un dueño designado, quien será responsable de asegurar que los mismos se encuentren debidamente protegidos.

Existe un proceso de gestión y repuesta de incidentes que establece las actividades para gestionarlos durante todo su ciclo de vida y se prueban al menos una vez al año.

Existe un programa de sensibilización y capacitación en temas de seguridad de la información, ciberseguridad y cumplimiento de la norma PCI DSS. Este programa se encuentra disponible para todo el personal de Proyectum, incluyendo empleados permanentes, temporales y externos.

La dirección de Proyectum declara su decisión de mejorar continuamente los procesos y niveles de seguridad a través de un seguimiento permanente de los controles y procedimientos implementados. Del mismo modo, declara su intención de asegurar la existencia de planes de contingencia que permitan garantizar la continuidad de los servicios prestados por la compañía.

La dirección de la Proyectum declara su decisión de cumplir con la normativa y legislación vigente en temas de Seguridad de la Información y con los requerimientos contractuales establecidos por los clientes con relación a la misma.

Existe un Inventario de los activos de la información con todos los dispositivos, softwares e información a la que acceden los colaboradores de Proyectum.

Todas las altas, bajas y modificaciones en los accesos de los colaboradores de Proyectum a los sistemas propios de la empresa como de sus clientes, cuentan con autorizaciones documentadas.

Todos los computadores que utilizan los colaboradores de Proyectum mantienen implementado un antivirus actualizado con monitoreo continuo.

Todas las conexiones remotas hacia los clientes de Proyectum, es utilizando un MFA (multifactor de autenticación), provisto por el cliente.

Existe implementado un proceso de accesos que incluye la definición de políticas de contraseñas a los accesos a los sistemas de Proyectum

Existe implementado un programa anual de cumplimiento PCI DSS, el cual detalla los responsables y actividades a realizar para el cumplimiento de Proyectum.

Existe implementado un proceso de gestión de riesgos operacionales para cubrir los ámbitos de seguridad de la información y ciberseguridad.

Existe implementado un proceso que gestiona los parches de seguridad y vulnerabilidades de los activos de Proyectum.

La responsabilidad de los respaldos de la información de los sistemas de negocio de Proyectum, son realizados por los proveedores de las soluciones SaaS. Proyectum, no administra ni mantiene infraestructura tecnológica.

Queda prohibido a los colaboradores realizar actividades de hacking sobre las plataformas tecnológicas de Proyectum y/o de sus clientes, a menos que se tenga un acuerdo por escrito que autoricen realizar dichas actividades.

Queda prohibido acceder, eliminar y/o alterar la información de Proyectum y/o de sus clientes, sin contar con la autorización para realizar dichas actividades.

Para la adquisición, mantención o desarrollo de software por terceros se debe considerar que el proveedor cumpla con un estándar de ciberseguridad, como por ejemplo OWASP TOP 10, como también considerar la propiedad de los códigos fuentes y responsabilidades con el licenciamiento del software.

GOBIERNO

Proyectum, establece una estructura de gobierno que permite implementar y mantener el proceso de Gestión de la Seguridad de la Información en base a las directrices de la presente política.

Dicha estructura cumple con las siguientes directrices:

- Definición de Roles y responsabilidad
- Aplicación de los controles de accesos a la información
- Protección de los medios de transmisión
- Definir controles para proveedores que tengan acceso a la información
- Gestionar los incidentes que puedan afectar la información o la continuidad de las operaciones de la empresa
- Aplicar controles que garanticen la realización segura de las actividades propias de la gestión de la información.

COMPROMISOS DE LA ALTA DIRECCIÓN

La Gerencia General de Proyectum, está comprometida con la presente Política de Seguridad de la Información y Ciberseguridad y con las exigencias establecidas en ella y adoptará las medidas suficientes y/o necesarias, para asegurar el cumplimiento de esta política, de conformidad a los objetivos de la empresa y a las normas legales vigentes.

ROLES Y RESPONSABILIDADES

ROL/CARGO	ACCIONES
Gerente General	• Aprobación anual de la política • Proveer los recursos necesarios para implementar la política • Conocer mensualmente el estado de la implementación y cumplimiento de la política • Definir los niveles de tolerancia a los riesgos • Firmar las excepciones a la presente política cuando corresponda • Liderar la implementación de la política
Oficial de Seguridad de la Información (CISO)	• Actualización anual de la política o ante cada evento que lo amerite • Reportar mensualmente los avances de la implementación de la norma PCI DSS • Coordinar las capacitaciones para colaboradores y proveedores • Centralizar las fallas, incidentes o incumplimientos a la política • Solicitar firmas a las excepciones de la presente política cuando corresponda
Gerente de Personas	• Coordinar capacitar ante cada contratación y al menos una vez al año. • Entregar una copia de la política a los colaboradores al inicio de cada contratación. • Comunicar la política a colaboradores • Ejecutar las sanciones definidas para el incumplimiento de la política, estipuladas en el Reglamento de Orden, Higiene y Seguridad
Gerente de Finanzas	• Actualizar y distribuir el Reglamento de Orden, Higiene y Seguridad
Asesores Jurídicos	• Entregar la asesoría legal respecto a los incumplimientos de la presente política
Todos los Colaboradores y Prestadores de Servicios	• Proteger la información de Proyectum y de sus clientes. • Comunicar al CISO cualquier falla, incidente o incumplimiento a la política

REFERENCIAS NORMATIVAS

La organización utiliza como referencia la norma ISO 27.001 “Sistema de Gestión de Seguridad de la Información” y la norma PCI DSS “PAY CARD INDUSTRY”