Política de Seguridad de la Información

Fecha: 08/08/2021

Elaboró:

Ernesto Rován

CTO

Aprobó:

Hugo Sacchi

CEO

2innovate
IT Solutions & Creativity

Tabla de contenidos

1 Objetivo

El presente documento define:

- Lineamientos que deben ser cumplidos por los empleados de 2innovateIT. Los terceros involucrados (proveedores, contratistas, otros) deben ser incluidos en los requerimientos de esta Política de manera obligatoria.
- Establecer un marco de trabajo para todos los procesos y sus mecanismos de seguridad.
- Clasificar la información y definir principios fundamentales para asegurarla de acuerdo con los objetivos del negocio en el ámbito de la seguridad de la información.
- Requerimientos mínimos para el gerenciamiento de la Información, Control de Accesos, Seguridad Física, Comunicaciones, Operaciones y Desarrollo de Sistemas.

2 Alcance

Esta Política se aplica a:

- Toda la información que es creada, recibida, almacenada, procesada, transmitida, entregada y descartada, usando cualquier sistema o medio de almacenamiento.
- La Compañía y sus empleados, así como a personal externos y/o proveedores que interactúan directa o indirectamente y a los clientes.

3 Política

3.1 Roles y Responsabilidades

Ciertas tareas privilegiadas o sensibles deben ser separadas de otras similares, para minimizar el riesgo de abuso de privilegio y para maximizar la habilidad de quienes tienen la función de controlar las tareas de los otros.

Respetando el principio de segregación de funciones, algunos roles deben ser ejercidos por distintos individuos o grupos, como, por ejemplo: administración del acceso o control sobre los sistemas operativos, uso normal de los sistemas y aplicaciones, auditoría y administración de la seguridad.

3.1.1 Usuarios

Los usuarios deben ser informados regularmente sobre el marco normativo existente, y deben recibir capacitación cuando sea necesario.

La concienciación sobre la seguridad podrá efectuarse mediante múltiples métodos de comunicación y educación hacia el personal (por ejemplo: carteles, cartas, memos, formación basada en la web, reuniones, otros).

El nuevo personal que se incorpore a 2innovateIT debe ser instruido respecto de la sensibilidad de los sistemas de información. Debe ser creada y mantenida una concientización en materia de ciberseguridad. La misma debe ser impartida al menos una vez al año.

3.1.2 Clientes

Los clientes no deberán dar ninguna contraseña que le suministre 2innovate. La empresa nunca le solicitará dicha información.

Si un empleado le pide información confidencial, debe ser por medios del correo @2innovateit.com o por los contactos de la web www.2innovateit.com esta no debe contener datos de tarjeta, contraseñas o claves de Home Banking.

Ante cualquier consulta enviar un mail a seguridad-informatica@2innovateit.com

3.1.3 Terceros involucrados

Los terceros involucrados se deben atener a los lineamientos establecidos por esta Política.

3.2 Análisis de Riesgo y Clasificación de la Información

Se debe realizar un adecuado análisis y clasificación de riesgos, el mismo debe identificar las amenazas, vulnerabilidades relacionadas a la información y realizarse, como mínimo, anualmente.

Algunas metodologías de evaluación de riesgos a considerar pueden ser: OCTAVE, ISO-IEC 31000, ISO-IEC 27005 y NIST SP 800-30, entre otras.

La información debe ser clasificada, según su nivel de clasificación.

3.3 Control de Acceso

La política de acceso de 2innovateIT está basada en el menor privilegio posible, es decir que a los usuarios que necesiten acceso se le dará el menor nivel de privilegio posible para cumplir sus funciones laborales.

Los recursos informáticos puestos por 2innovateIT a disposición de los usuarios están destinados a ser utilizados en el desarrollo de las actividades diarias.

2innovateIT se reserva el derecho de acceder a todos los equipos y sistemas utilizados en el desarrollo de sus negocios, con fines de soporte operacional y/o para la protección de sus activos.

3.3.1 Lineamientos de Negocios para el Control de Accesos

Los sistemas de información y redes deben tener mecanismos de seguridad definidos e implementados, para proveer un nivel apropiado de protección a la información que maneja.

Para que un usuario tenga acceso a los sistemas o aplicaciones, sus derechos de acceso deben ser autorizados y su identidad verificada por al menos su superior directo o un directivo/gerente de la compañía.

Se deben utilizar mecanismos de auditoría operativa para controlar la utilización de los derechos de acceso a las aplicaciones y para asegurar que el nivel de acceso otorgado es consistente con las funciones de cada usuario.

Los usuarios deben ser responsables del uso otorgado de sus dispositivos y datos de autenticación (usuarios, claves, PINs, otros).

Está prohibido compartir credenciales de acceso y dispositivos de autenticación, los mismos deben ser mantenidos en secreto y seguros.

Los accesos a los sistemas son monitoreados para asegurar el cumplimiento de las normas de acceso.

3.4 Seguridad física de la información

Todos los recursos informáticos que son críticos para la continuidad de los negocios de 2innovateIT deben ser físicamente asegurados.

El acceso físico a la infraestructura de redes y comunicaciones debe estar limitado a los usuarios autorizados.

Cada vez que el personal deje su oficina o escritorio, se debe asegurar que ninguna información confidencial u otro material sensitivo queden desprotegidos.

3.5 Protección contra software malicioso

La empresa provee herramientas adecuadas para la protección de los equipos informáticos contra amenazas de malware.

Los usuarios deben seguir las prácticas de seguridad para minimizar el riesgo, como por ejemplo no utilizar software no autorizado o no abrir mensajes de correo electrónico de origen desconocido o dudoso.

3.6 Clasificación de la información

Toda la información en formato físico, escrita o impresa debe estar clasificada de acuerdo con sus requerimientos de seguridad.

La política de clasificación se basa en los siguientes 3 niveles:

- Nivel 1 – Información pública
- Nivel 2 – Información reservada
- Nivel 3 – Información confidencial

3.7 Destrucción de información

El descarte de los medios de almacenamiento de información de cualquier tipo tiene un tratamiento acorde con el nivel de clasificación del dato almacenado.

Para el caso de la información sensible el medio debe ser físicamente destruido o debidamente borrado en el caso que se lo pretenda reutilizar.

3.8 Correo electrónico uso para negocios

Los sistemas de correo electrónico de 2innovateIT deben ser utilizados para fines de negocios.

El uso personal se encuentra permitido en la medida que:

- No consuma recursos significativos.
- No entorpezca cualquier actividad de negocios.

Está prohibido a los empleados el uso de cualquier sistema de correo electrónico que no sea de 2innovateIT para enviar o recibir información relacionada con los negocios de 2innovateIT.

Todos los mensajes enviados desde 2innovateIT deben cumplir con esta política, la legislación local y los estándares de la Compañía en cuanto al contenido.

La información confidencial o estrictamente confidencial no debe ser enviada por correo electrónico, a menos que sea encriptada según estándares autorizados.

3.9 Internet

Los empleados de 2innovateIT pueden ser provistos de acceso a Internet para asistirlos en el desarrollo de su trabajo.

El uso de Internet debe ser específicamente enfocado a las tareas que el usuario desarrolla dentro de la Compañía, un uso personal está permitido dentro de límites razonables y siempre que los sitios accedidos no sean ilegales o inapropiados para un ambiente de trabajo bien controlado (por ejemplo: sitios relacionados con pornografía, juego, drogas, otros).

El uso de Internet no debe ser utilizada para violar derechos de propiedad intelectual o cualquier sistema informático o redes.

El acceso a otros recursos que no sean páginas de Internet está reservado a usuarios autorizados.

La descarga de archivos electrónicos desde Internet no está permitida, salvo que sea una parte necesaria del trabajo del Usuario.

3.10 Transferencia de archivos

La información sensible no debe ser enviada a través de ningún mecanismo de transferencia de archivos, a menos que sea encriptada de acuerdo con los estándares de 2innovateIT.

3.11 Acceso remoto

El acceso que realice el personal de 2innovateIT a los recursos de la Compañía por fuera de la red interna debe ser realizado a través del mecanismo de Acceso Remoto seguro como VPN o enlaces dedicados.

3.12 Puesta a producción

El software debe ser puesto en producción de manera controlada. Todos los sistemas en producción deben tener un versionado y su respectivo control de cambios.

Las tareas y responsabilidades claves en el entorno de producción, deben ser segregadas para garantizar la debida oposición de intereses y minimizar el abuso de funciones privilegiadas.

La efectividad de los mecanismos de seguridad diseñados en los sistemas debe ser controlada a través de un testeo de seguridad formal, antes de ser puestos en producción, y verificada regularmente.

Todo software de terceras partes debe ser obtenido de fuentes confiables y debe ser utilizado estrictamente de acuerdo con los términos de la licencia. El derecho de propiedad intelectual del software debe ser respetado y observado en todos los casos.

3.13 Desarrollo de software

El desarrollo y el mantenimiento del software que se utilice en 2innovateIT deben seguir las normas de seguridad definidas por la Compañía.

Los requerimientos y el diseño de seguridad deben ser compatibles y estar integrados con el diseño de seguridad existente para las redes y sistemas de 2innovateIT.

Los entornos de desarrollo, testing y producción deben ser segregados.

Cualquier acceso de este tipo debe ser otorgado en circunstancias excepcionales, ser temporario, justificado y registrado.

Los empleados involucrados en el desarrollo de software deben ser entrenados en los aspectos de seguridad referentes a la evaluación, instalación y mantenimiento de los sistemas.

3.14 Conectividades de redes

Las redes de 2innovateIT deben ser protegidas contra accesos no autorizados.

Todas las redes de 2innovateIT deben ser clasificadas en confiables y no confiables de acuerdo con el nivel de seguridad que posean.

Todas las comunicaciones entre redes internas y externas (Por ejemplo: Internet) o entre áreas de red con clasificación de seguridad variable, deben ser salvaguardadas a través de dispositivos de seguridad.

Deben aplicarse mecanismos de seguridad adecuados, en el punto de conexión cuando se conecte con una red de terceras partes, una red pública o un segmento de red interna no confiable.

3.15 Respuesta ante incidentes

La empresa actúa ante situaciones o eventos donde se haya comprometido o se pueda comprometer los sistemas. Este tiene la capacidad de detectar intrusiones, realizar tareas de rastreo e identificación y análisis forense sobre los sistemas informáticos en donde se hayan producido los incidentes.

3.16 Continuidad del procesamiento

La empresa realiza gestión de riesgo que amenazan la continuidad del procesamiento de la información crítica para el funcionamiento del negocio y en consecuencia implementa controles preventivos y planes de recuperación para reducirlos a niveles aceptables.

3.17 Uso de tecnologías críticas

Para el uso de Tecnologías críticas se debe tener en cuenta los siguientes aspectos:

- Todos los activos deben estar inventariados y aceptadas/aprobadas por la institución.
- Debe tener autenticación segura para el uso de la tecnología críticas.
- Debe tener un responsable en caso de que exista alguna necesidad de tratamiento o uso del activo.
- La activación de las tecnologías de acceso remoto para proveedores y socios de negocio debe hacerse sólo cuando sea necesario, con desactivación inmediata después de su uso.
- No se debe utilizar ningún medio extraíble no autorizado. Estos pueden contener software malicioso que podría afectar la seguridad de la compañía.

3.18 Política a proveedores

Los proveedores que ingresan a los activos de la empresa deben cumplir con al menos las siguientes políticas de seguridad:

- Tener un convenio de confidencialidad o cláusula de confidencialidad en contrato.
- Cumplir con las políticas de seguridad que les apliquen.
- Estar certificados de acuerdo con las normas o regulaciones de seguridad que les aplique o aceptar revisiones/auditorias en caso de ser necesario.

- Responsabilidad de avisar de cualquier incidente de seguridad.
- Responsabilidad en caso de daño reputacional o patrimonial a la institución por dolo o negligencia de su personal asignado.
- Proveer capacitación de seguridad a sus empleados asignados a la institución.

4 Historial de cambios

Fecha	Versión	Elaboró	Revisó y Aprobó	Detalle
08/08/2021	1	Ernesto Rován CTO	Hugo Sacchi CEO	Confección inicial del documento.