Política de Seguridad de la Infromación

2innovate

Contenido

Objetivo

El objetivo de este documento es especificar los requerimientos obligatorios mínimos para el uso adecuado y la protección de la información, además de proveer un marco para todas las actividades relacionadas con el Seguridad Informática dentro de 2innovateIT.

El objetivo de la política de seguridad es proteger la información, de manera que las obligaciones legales y contractuales de los negocios de 2innovateIT sean cumplidas y que el valor de los negocios y de su información sea preservado.

El objetivo de Seguridad Informática es garantizar:

- Confidencialidad: Prevenir que la información sea accedida por individuos, entidades o procesos no autorizados.
- Integridad: Proteger la información de la modificación, manipulación o reproducción no autorizada.
- Disponibilidad: Asegurar que toda la información y los servicios significativos para los negocios estén disponibles cuando sean requeridos, para los usuarios, entidades o procesos autorizados.
- No-Repudio: Asegurar que la información haya sido originada en determinado individuo, entidad o proceso.

La información es uno de los principales activos de los negocios de 2innovateIT. Toda la información sensible debe ser mantenida de manera confidencial, precisa y estar disponible, de la manera apropiada para cubrir las necesidades de los negocios.

Cada empleado debe ser consciente de la necesidad de asegurar la información y actuar para preservar la misma.

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.

2innovateIT es libre de definir e implementar requerimientos y mecanismos de seguridad más fuertes, siempre que no contradiga esta Política.

Cuando la política se vea afectada por leyes y/o regulaciones debe ser compatibilizada para que cumpla con las mismas, tratando en lo posible, que no distorsione las exigencias de 2innovateIT.

Esta Política debe ser sujeta a revisión como mínimo anualmente, o con mayor frecuencia según lo defina Seguridad Informática respecto a las necesidades de la Compañía.

El marco normativo debe estar accesible para el personal y los terceros involucrados; éste define los siguientes niveles de documentos:

- Política de Seguridad
- Normas
- Procedimientos/ Guías/ Estándares

Alcance

Esta Política se aplica a cada persona que desarrolle alguna actividad en 2innovateIT sin importar bajo cuáles condiciones (directivo, empleado, contratado, consultor, temporario, otros).

Política

1.1 Implementación de la Política de Seguridad

Se instrumenta a través de la publicación de Normas, Procedimientos, Guías o Estándares que se encuentran alineados y que complementan lo dispuesto en esta Política.

Dichos documentos deben ser publicados en lugares accesibles para los empleados. La publicación de estos debe ser acompañada de la notificación formal a los responsables de las áreas involucradas.

Todo documento publicado de acuerdo con lo indicado anteriormente entra en vigor al momento de la publicación.

1.2 Gerenciamiento

Para cumplir con el objetivo de Seguridad Informática es esencial que:

- La implementación de mecanismos de seguridad específicos se justifica en relación con los riesgos a los que está expuesta la información que está siendo protegida.
- Todos los empleados y terceros serán responsables de la manipulación de la información.
- Existan registros de eventos sobre las transacciones y cambios realizados a la información.
- Se efectúe un examen independiente de la administración y uso de la información.

1.3 Roles y Responsabilidades

1.3.1 Separación de 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.

1.3.2 Dueño de Datos

Las operaciones de 2innovateIT se sustentan en diversos conjuntos de datos o grupos de información, los cuales son gestionados en los diferentes sectores o unidades de negocios. Cada grupo de información debe tener un dueño de datos que sea designado por Seguridad Informática.

1.3.3 Usuarios

Los empleados 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, formación basada en la web, reuniones, otros).

Debe ser creada y mantenida una concientización en materia de ciberseguridad, gestionado por el Seguridad Informática. La misma debe ser impartida al menos una vez al año.

1.3.4 Terceros involucrados

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

1.3.5 Seguridad Informática

Este sector tiene las siguientes responsabilidades:

- Resolver posibles conflictos entre el marco normativo y la legislación del país o regulaciones de clientes.
- Coordinar las actividades e investigaciones respecto de incidentes de sistemas.
- Gestionar el programa de concientización.
- Evaluar permanentemente nuevas vulnerabilidades y mantener un nivel de seguridad razonable en relación con los bienes a proteger.
- Asesorar en aspectos relacionados con la seguridad cuando sean considerados en la selección de los contratistas.
- Monitorear el día a día de la implementación y uso de los mecanismos de los sistemas, incluyendo el acceso a la información.
- Administrar las cuentas de usuarios y gestionar la autenticación a los sistemas de información.

1.3.6 Auditoría

Evaluar si la consistencia de los mecanismos de seguridad implementados concuerda con los requerimientos y el diseño de seguridad. Estos controles abarcan a toda la organización.

1.4 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: ISO 31000, NIST SP 800-30, entre otras.

1.5 Control de Acceso

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.

1.5.1 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 manejan.

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 utilizan 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.

1.5.2 Gerenciamiento del Acceso de Usuario

Todos los recursos informáticos son provistos para su uso en los negocios de 2innovateIT y deben ser utilizados para ello, un uso personal razonable está permitido si cumple con las restricciones dictadas por esta Política, como ser:

- Se realiza fuera de su horario de trabajo para que no interfiera ni con su productividad, ni con la de otros empleados.
- No consuma recursos que compitan con la producción (ej. enlaces de Internet)
- No consuma recursos que signifiquen cargos para 2innovateIT (ej. comunicaciones, papel, medios magnéticos, otros).
- No signifique un riesgo legal a 2innovateIT (Por ejemplo: violación de derechos de autor u otro).

1.5.3 Control de Acceso al Sistema Operativo y las Aplicaciones

El acceso a los sistemas de información debe ser controlado y restringido a usuarios autorizados, de manera de minimizar el riesgo de accesos indebidos.

Los dispositivos de seguridad de una aplicación deben ser capaces de identificar y verificar la identidad de cada usuario autorizado, mediante mecanismos de autenticación definidos por Seguridad Informática.

1.5.4 Monitoreo del Acceso a los sistemas y su uso

Se debe implementar un adecuado monitoreo para asegurar que todos los eventos relacionados con la seguridad sean identificados y corregidos. Todas estas actividades de monitoreo deben ser consistentes con las regulaciones y legislación de privacidad vigentes en cada uno de los sitios en que actúa 2innovateIT.

Los accesos a los sistemas deben ser registrados y monitoreados para asegurar el cumplimiento de las normas de acceso.

1.6 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 empleados autorizados.

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

1.7 Protección contra Software Malicioso

Seguridad Informática debe proveer o controlar 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.

1.8 Intercambio de Información y Software

1.8.1 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 consume 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.

1.8.2 Mensajería instantánea

El uso de mensajería instantánea tiene que ser utilizado por hangout de Google, el cual está certificado en PCI-DSS.

1.8.3 Monitoreo de las Comunicaciones

Seguridad Informática se reserva el derecho de monitorear cualquier tráfico electrónico como parte de sus actividades operacionales normales, dentro del marco de la legislación vigente.

1.8.4 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 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.

1.8.5 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.

1.8.6 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 autorizado por 2innovateIT.

1.9 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.

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.

1.10 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 entornos de desarrollo y producción deben ser segregados. Cualquier acceso de este tipo debe ser otorgado en circunstancias excepcionales, ser temporario, justificado y registrado.

Los desarrollos pasan por diferentes estadios antes de pasar a producción.

1.11 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.

1.12 Respuesta ante incidentes

Seguridad Informática debe actuar ante situaciones o eventos donde se haya comprometido o se pueda comprometer los sistemas. Este debe tener 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.

1.13 Continuidad del Procesamiento

Se deben analizar los riesgos que amenazan la continuidad del procesamiento de la información crítica para el funcionamiento del negocio y se deben implementar controles preventivos y planes de recuperación para reducirlos a niveles aceptables.

La continuidad de la operación de los sistemas debe ser asegurada, mediante un adecuado Plan de Contingencias.

1.14 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 aceptados/aprobados por la institución.
- Debe tener autenticación segura para el uso de la tecnología crítica.
- Debe tener un responsable en caso de que exista alguna necesidad de tratamiento o uso del activo.
- Requerimiento de desconexión automática de sesiones para tecnologías de acceso remoto después de un período específico de inactividad.
- 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.
- Los ambientes cloud no tienen necesidad de tener activadas las unidades virtuales de medios extraíbles en sus sistemas, el cual tendrá que estar desactivado.

1.15 Cifrado en base de datos

La política de la empresa es cifrar los datos confidenciales a nivel base de datos con un cifrado seguro y manejo adecuado de las llaves de cifrado de dichos datos.

1.16 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 el contrato.
- Estar certificados PCI o aceptar revisiones/auditorías en caso de ser necesario.
- Responsabilidad de avisar de cualquier incidente de seguridad.
- Responsiva 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.

1.17 Política de borrado seguro

Para todos los sistemas se tiene implementado un proceso de borrado seguro para asegurarse que la información no puede ser recuperable.

1.18 Política a actualizaciones

Todo software debe estar actualizado a su última versión estable. Puede ocurrir que el mismo no esté en su última versión por cuestiones de inestabilidad o rendimiento, no obstante, se debe tener identificado sus vulnerabilidades en dicha versión y analizar el impacto en los sistemas.