Política de Seguridad de la Información

Septiembre 2024

#SomosUfinet

Política de Seguridad de la Información

Introducción

Ufinet reconoce la importancia y el valor que posee la información con respecto al funcionamiento eficiente y efectivo de la organización. La información no es sólo crítica para el éxito de la organización, sino estratégica para su sostenibilidad a largo plazo. Por este motivo, Ufinet toma acciones apropiadas para proteger los activos de información contra amenazas que podrían conducir a la pérdida, modificación o divulgación de estos.

Esta Política establece los principios, lineamientos y directrices generales que rigen la gestión de la seguridad de la información en Ufinet, basándose en el estándar internacional ISO/IEC 27001:2022, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de Ufinet.

¿Qué es Confidencialidad?

Es la protección de la información contra el acceso no autorizado.

¿Qué es Integridad?

Es la protección de la información contra la modificación no autorizada.

¿Qué es Disponibilidad?

Es la garantía de que la información esté disponible para los usuarios autorizados cuando lo requieran.

Política de Seguridad de la Información

Alcance

Esta Política, sus normas y procedimientos relacionados se aplican a toda la información, recursos y tecnologías de Ufinet, sin importar su formato o ubicación. Esto significa que las reglas y directrices establecidas aplican a todos los datos y recursos de Ufinet, incluyendo, pero no limitado a, documentos físicos y digitales, sistemas informáticos, software, hardware, y cualquier otra forma de información o tecnología utilizada en Ufinet.

Además de lo anterior, su aplicabilidad se extiende a todos sus empleados, colaboradores y socios comerciales, independientemente de su nivel o función.

Esta Política establece directrices claras, prácticas y sólidas que rigen el uso responsable, seguro y eficiente de la información y las tecnologías para respaldar de manera efectiva las operaciones de Ufinet, garantizando la confidencialidad, integridad y disponibilidad de los activos de información. Adicionalmente, promueve prácticas que reduzcan los riesgos, cumplan con los requisitos legales y contractuales relacionados y salvaguarden los intereses de Ufinet y sus clientes.

Además, contribuye a la gestión eficaz del Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de asegurar los siguientes objetivos:

- Garantizar la seguridad del personal y de los activos de Ufinet.
- Minimizar las molestias a clientes y socios comerciales, protegiendo así la reputación y prestigio de Ufinet.

Política de Seguridad de la Información

Líneas de Actuación Prioritarias

Esta política establece directrices para:

- Desarrollar y perfeccionar un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la norma ISO 27001 para proteger eficazmente los activos de información.
- Cumplir, en todas las actividades y ubicaciones, los requisitos legales, reglamentarios y contractuales que puedan afectar a la seguridad de la información.
- Identificar y responder a los requisitos de seguridad, teniendo en cuenta las necesidades y expectativas de nuestros clientes, socios comerciales, empleados y colaboradores y otras partes interesadas.
- Llevar a cabo actividades de evaluación y mitigación de riesgos para reducir la probabilidad y el impacto de un incidente mediante medidas proactivas, abordando e identificando los riesgos con antelación.
- Desarrollar estrategias y procedimientos para garantizar una respuesta eficaz ante cualquier incidente de seguridad, teniendo siempre como máxima prioridad la salud y la seguridad de las personas.
- Garantizar una estructura de apoyo con herramientas y recursos que permitan una respuesta eficaz ante incidentes de seguridad de la información.
- Garantizar que nuestros empleados y otras partes interesadas estén adecuadamente informados, sensibilizados y formados en relación con la importancia de la seguridad de los activos de Ufinet.
- Garantizar que el SGSI está actualizado y es eficaz, y que las medidas adoptadas funcionarán según lo previsto y siempre que sea necesario.

Política de Seguridad de la Información

Organización

Ufinet está firmemente comprometida con la seguridad de la información. Por tanto, cada miembro de la organización comprende su función específica y sus responsabilidades dentro del Sistema de Gestión de Seguridad de la Información (SGSI). Los siguientes puntos son considerados cruciales para un desempeño eficaz:

- **Asignación de Responsabilidades:** Ufinet se asegurará de que las responsabilidades y autorizaciones relacionadas con la seguridad de la información se asignen y comuniquen debidamente.
- **Responsabilidad de Conformidad:** Se designará a personas responsables de garantizar que el SGSI cumpla con los requisitos de esta Política.
- **Informes de Desempeño:** La responsabilidad de informar sobre el desempeño del SGSI se establecerá mediante comités de seguimiento.

Política de Seguridad de la Información

1. Organización interna

La seguridad de la información debe estar conformada por los siguientes actores, a quienes se les definirán roles y responsabilidades:

- **Comité de Dirección:** Deberá aprobar la Política de Seguridad de la Información, velar por la adecuada asignación de los recursos necesarios para mantener una correcta gestión de la seguridad de la información y promover una cultura de seguridad en Ufinet
- **Comité de Seguridad de la Información (CyberCom):** Deberá administrar las iniciativas sobre seguridad de la información, a través de compromisos apropiados y del uso de recursos adecuados en Ufinet, así como la formulación y actualización de esta Política
- **Chief Information Security Officer (CISO):** Será el responsable de supervisar todas las actividades relacionadas con la seguridad de la información, garantizando la protección de los activos de información de Ufinet contra amenazas internas y externas, asegurando la protección adecuada de los activos de información y la mitigación efectiva de los riesgos de seguridad
- **Encargado de Seguridad de la Información:** Será el responsable de la implementación, operación, mantenimiento y mejora transversal de esta Política, sus normas y procedimientos relacionados

Política de Seguridad de la Información

2. Segregación de funciones

Ufinet priorizará la confiabilidad, disponibilidad, confidencialidad y auditoría de sus sistemas. Esto implica mantener sistemas seguros y accesibles, proteger la información, permitir la revisión de actividades y evitar conflictos entre las diferentes tareas. Por ello, las responsabilidades se encontrarán claramente definidas y documentadas, y se implementarán controles de autorización necesarios. Además, se efectuarán revisiones periódicas para mantener la segregación de funciones y minimizar riesgos.

3. Contacto con Autoridades y Grupos Especiales de Interés

El área de Seguridad de la Información de Ufinet establecerá y mantendrá contacto con las autoridades nacionales e internacionales que pudieran dar soporte, información, ayuda o lineamientos relacionados a la seguridad de la información, lo cual implica:

- Identificar entidades que representen una figura de apoyo y autoridad en temas de seguridad de la información y afines
- Revisar y estudiar las nuevas normas y requerimientos que las autoridades establezcan en relación con la seguridad de la información
- Adoptar los requerimientos existentes, previa aprobación del CyberCom

Política de Seguridad de la Información

4. Seguridad de la Información en la Gestión de Proyectos

Con el objetivo de proteger nuestra información confidencial, ampliar la confianza de nuestros clientes, reducir el riesgo de incidentes de seguridad de la información y mejorar nuestra eficiencia y productividad, Ufinet integrará la seguridad de la información a aquellos procesos de gestión de proyectos que pudieran afectar la confidencialidad, integridad y disponibilidad de la información. Integrar la gestión de seguridad de la información desde el comienzo de los proyectos permite abordar oportunamente los problemas de seguridad desde la fase de diseño del producto o servicio. Esto hace que el proceso de implementación sea más eficiente y asegura que los riesgos sean identificados y gestionados de manera efectiva desde el principio.

5. Dispositivos Móviles y Teletrabajo

La información de Ufinet podría estar en peligro en entornos externos que no estén bajo su control, motivo por el cual se define un marco de uso y control sobre los dispositivos móviles y el trabajo remoto, definiendo reglas de seguridad relacionadas para salvaguardar los activos de Ufinet.

Política de Seguridad de la Información

Seguridad de las Personas

En Ufinet, se reconoce que la seguridad de la información es una responsabilidad compartida y, por tanto, es fundamental promover una cultura de conciencia de seguridad. Para lograr esto, se implementarán una serie de estrategias. Se proporcionará capacitación inicial y periódica a todos los empleados y colaboradores, adaptada a sus roles y responsabilidades, que incluirá la comprensión de esta Política, sus normas y procedimientos relacionados. Además, se fomentará la conciencia de seguridad a través de diversos medios, como sesiones de capacitación y boletines informativos.

Regularmente, se comunicará la importancia de la seguridad de la información y se reafirmará el compromiso con la protección de los activos de información. También se fomentará la sensibilización a través de campañas internas y se establecerá un canal de comunicación para que los empleados y colaboradores puedan reportar incidentes de seguridad.

En este marco, **cada empleado asume la responsabilidad de proteger la información y los activos de Ufinet, de reportar incidentes de seguridad de la información y de cumplir con esta Política**.

Para medir la efectividad de las actividades de capacitación y concienciación, se realizarán evaluaciones periódicas de la conciencia de seguridad, con el fin de identificar áreas de mejora.

Política de Seguridad de la Información

Gestión de Activos

Con el fin de salvaguardar los activos de información de Ufinet, se establecerá un proceso de gestión de activos para determinar las responsabilidades, impulsar la clasificación de la información y definir las medidas para proteger los activos de información contra el acceso no autorizado, su pérdida o destrucción y su corrupción.

Cada activo contará con un propietario, que será responsable de definir la adecuada utilización y asegurar que dicho activo esté debidamente protegido.

Control de Acceso

Ufinet priorizará el establecimiento de un control de acceso adecuado para proteger su información, mejorar su eficiencia y seguridad, y minimizar los riesgos de incidentes de seguridad de la información. Los permisos de acceso se asignarán según roles y responsabilidades, y se realizarán controles regulares para evitar accesos indebidos. Todos los empleados deberán ser conscientes de su responsabilidad en el uso de la información y los sistemas de Ufinet.

Criptografía

Fiel a su compromiso de protección de datos, Ufinet establecerá y definirá los requisitos en el uso de criptografía, incluyendo información a cifrar, algoritmos de cifrado robusto, longitud de claves a utilizar y métodos de gestión de claves.

Política de Seguridad de la Información

Seguridad Física y del Entorno

Para proteger los activos de información contra el acceso no autorizado, su pérdida o destrucción y su corrupción, Ufinet implementará diversas medidas preventivas y de monitoreo que comprenden, y no se limitan a, el control de acceso físico de las instalaciones y los sectores críticos, la seguridad de las personas, la seguridad de los activos fuera de las instalaciones, la seguridad perimetral, la seguridad de las instalaciones tecnológicas, la protección ante incendios y desastres naturales, la seguridad del ambiente, la eliminación segura de activos, los equipos desatendidos y los escritorios limpios.

Seguridad de las Operaciones

Ufinet priorizará la seguridad y las operaciones de sus sistemas mediante la documentación de procedimientos, la gestión de los cambios, la separación de ambientes, los controles contra código malicioso, la instalación adecuada de los sistemas operativos y la gestión de vulnerabilidades. Además, se asegurará de realizar copias de seguridad y de registrar y monitorizar las disrupciones.

Seguridad de las Comunicaciones

La seguridad de las comunicaciones es esencial para proteger la información. Por ello, se implementarán medidas como la encriptación de comunicaciones y redes, la segregación de redes para evitar amenazas, el filtrado de páginas web, la identificación de la clasificación de la información transmitida, la encriptación de información confidencial y la protección de dispositivos móviles. Además, será crucial definir acuerdos claros sobre la información compartida con terceros.

Política de Seguridad de la Información

Contratación, Desarrollo y Mantenimiento de Sistemas

Ufinet reconoce la importancia y trascendencia de los sistemas en su estrategia de negocio, así como su interés en asegurar que los proyectos y sistemas tecnológicos sigan las mejores prácticas de seguridad durante el proceso de contratación, desarrollo y mantenimiento de los mismos. Por ello, se considerará esencial la participación del área de Seguridad de la Información desde el inicio de los proyectos, así como en la definición de requisitos de seguridad para el desarrollo de aplicaciones, el ciclo de vida para el desarrollo seguro, la instauración de la gestión de cambios de los sistemas y la implementación de una arquitectura de sistemas basada en la seguridad y en principios de ingeniería. También se dará importancia a la codificación segura, la separación de entornos, el control sobre desarrollos de terceros y la protección adecuada para los datos contenidos en los ambientes de pruebas.

Relación con Socios Comerciales

La necesidad de establecer y mantener relaciones seguras con nuestros socios comerciales es parte relevante y fundamental en la estrategia del negocio. Por esta razón, se establecerán las pautas necesarias de seguridad en la relación con socios comerciales, teniendo en cuenta aspectos importantes como evaluaciones de riesgos vinculados a la contratación del socio comercial y su capacidad para cumplir con los requisitos de seguridad de Ufinet.

Política de Seguridad de la Información

Gestión de Incidentes de Seguridad de la Información

Ufinet comprende la importancia de responder adecuadamente a posibles incidentes de seguridad de la información que puedan afectar su operativa. Por ello, además de establecer controles de seguridad para minimizar la probabilidad de un incidente, implementará procedimientos que permitan dar una respuesta diligente ante diferentes escenarios.

Seguridad de la Información en la Gestión de Continuidad de Negocio

Un incidente de seguridad, como una violación de datos o un ataque cibernético, puede tener un impacto significativo, afectando seriamente nuestra operación. Esto podría resultar en pérdidas de datos, interrupción de servicios, daño a nuestra reputación y potenciales sanciones legales. Por ello, una adecuada gestión de la continuidad del negocio es vital para garantizar que nuestras operaciones críticas puedan continuar durante y después de un incidente de seguridad. Ufinet se asegurará de que la continuidad del negocio sea planificada, implementada, probada periódicamente y evaluada, con el fin de asegurar su eficacia al momento de ponerla en acción ante un evento disruptivo.

Política de Seguridad de la Información

Consecuencias de Infracciones

Ufinet podría enfrentarse a graves sanciones penales y civiles, así como a daños a su reputación, por el incumplimiento de esta Política. Ufinet también podría incurrir en costes significativos asociados a la investigación de dichos incidentes, quedar excluida de contratación pública y ser objeto de demandas civiles por parte de accionistas, clientes y competidores.

Los empleados que infrinjan esta Política estarán sujetos a medidas disciplinarias que pueden incluir el despido. Además, podrán ser considerados personalmente Ufinet podrá remitir las sospechas de infracción a las autoridades o reguladores competentes, lo que podría acarrear sanciones, multas y/o penas de prisión para los empleados que sean declarados culpables de infringir la ley.

Si el Comité de Integridad Empresarial (BIC, por sus siglas en inglés) determina que un tercero no ha cumplido las disposiciones de esta Política, Ufinet tomará las medidas oportunas, que pueden incluir la rescisión del contrato del tercero, el inicio de las acciones legales pertinentes y/o la notificación a las autoridades competentes en relación con la infracción.

¿Cómo puedo plantear una inquietud?

Consulte la Política de Denuncia de Irregularidades para saber cómo informar adecuadamente de cualquier conducta que pueda constituir una potencial infracción de esta Política o para plantear una inquietud.

ufinet

Política de Seguridad de la Información

Aprobación y Actualización

La aprobación de esta Política será efectuada por el Comité de Dirección. Así mismo, será revisada al menos una vez al año o siempre que se produzcan cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

Versiones

- Versión 1.0. Septiembre 2024. Elaborado por Luis Román / Ignacio Ortiz. Revisado por Álvaro de Pablo. Aprobado por ExCo.

#SomosUfinet