Política de seguridad de la información y SGSI

Política de seguridad de la información

1. **Resumen de la política**: La información debe ser siempre protegida, cualquiera que sea su forma de ser compartida, comunicada o almacenada.
2. **Introducción**:
    0. La información puede existir en diversas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en proyecciones o en forma oral en las conversaciones.
    1. La seguridad de la información es la protección de la información contra una amplia gama de amenazas con el fin de garantizar la continuidad del negocio, minimizar los riesgos empresariales y maximizar el retorno de las inversiones y oportunidades de negocio.
3. **Alcance**:
    0. Esta política apoya la política general del Sistema de Gestión de Seguridad de la Información de la organización.
    1. Esta política es de consideración por parte de todos los miembros de la organización.
4. **Objetivos de seguridad de la información**:
    0. Comprender y tratar los riesgos operacionales y estratégicos en seguridad de la información para que permanezcan en niveles aceptables para la organización.
    1. La protección de la confidencialidad de la información relacionada con los clientes y con los planes de desarrollo.
    2. La conservación de la integridad de los registros contables.
    3. Los servicios Web de acceso público y las redes internas cumplen con las especificaciones de disponibilidad requeridas.
    4. Entender y dar cobertura a las necesidades de todas las partes interesadas.
5. **Principios de seguridad de la información**:
    0. Esta organización afronta la toma de riesgos y tolera aquellos que, en base a la información disponible, son comprensibles, controlados y tratados cuando es necesario. Los detalles de la metodología adoptada para la evaluación del riesgo y su tratamiento se encuentran descritos en la política del SGSI.
    1. Todo el personal será informado y responsable de la seguridad de la información, según sea relevante para el desempeño de su trabajo.
    2. Se dispondrá de financiación para la gestión operativa de los controles relacionados con la seguridad de la información y en los procesos de gestión para su implantación y mantenimiento.
    3. Se tendrán en cuenta aquellas posibilidades de fraude relacionadas con el uso abusivo de los sistemas de información dentro de la gestión global de los sistemas de información.
    4. Se harán disponibles informes regulares con información de la situación de la seguridad.
    5. Los riesgos en seguridad de la información serán objeto de seguimiento y se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable.
    6. Los criterios para la clasificación y la aceptación del riesgo se encuentran referenciados en la política del SGSI.
    7. Las situaciones que puedan exponer a la organización a la violación de las leyes y normas legales no serán toleradas.
6. **Responsabilidades**:
    0. El equipo directivo es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la organización.
    1. Cada gerente es responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.

2. El responsable de seguridad asesora al equipo directivo, proporciona apoyo especializado al personal de la organización y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.
3. Cada miembro del personal tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

7. **Indicadores clave**:
    0. Los incidentes en seguridad de la información no se traducirán en costes graves e inesperados, o en una grave perturbación de los servicios y actividades comerciales.
    1. Las pérdidas por fraude serán detectadas y permanecerán dentro de unos niveles aceptables.
    2. La aceptación del cliente de los productos o servicios no se verá afectada negativamente por aspectos relacionados con la seguridad de la información.
8. **Políticas relacionadas**: A continuación, se detallan aquellas políticas que proporcionan principios y guía en aspectos específicos de la seguridad de la información:
    0. Política del Sistema de Gestión de Seguridad de la Información (SGSI).
    1. Política de control de acceso físico.
    2. Política de limpieza del puesto de trabajo.
    3. Política de software no autorizado.
    4. Política de descarga de ficheros (red externa/interna).
    5. Política de copias de seguridad.
    6. Política de intercambio de información con otras organizaciones.
    7. Política de uso de los servicios de mensajería.
    8. Política de retención de registros.
    9. Política sobre el uso de los servicios de red.
    10. Política de uso de informática y comunicaciones en movilidad.
    11. Política de teletrabajo.
    12. Política sobre el uso de controles criptográficos.
    13. Política de cumplimiento de disposiciones legales.
    14. Política de uso de licencias de software.
    15. Política de protección de datos y privacidad.

En un nivel inferior, **la política de seguridad de la información debe ser apoyada por otras normas o procedimientos** sobre temas específicos que obligan aún más la aplicación de los controles de seguridad de la información y se estructuran normalmente para tratar las necesidades de determinados grupos dentro de una organización o para cubrir ciertos temas.

Ejemplos de estos temas de política incluyen:

1. Control de acceso.
2. Clasificación de la información.
3. La seguridad física y ambiental.

Y más directamente dirigidas a usuarios:

1. El uso aceptable de los activos.
2. Escritorio limpio y claro de la pantalla.
3. La transferencia de información.
4. Los dispositivos móviles y el teletrabajo.
5. Las restricciones a la instalación de software y el uso.
6. Copia de seguridad.
7. La transferencia de información.
8. La protección contra el malware.
9. La gestión de vulnerabilidades técnicas.

10. Controles criptográficos.
11. Las comunicaciones de seguridad.
12. La intimidad y la protección de la información personal identificable.

Estas políticas/normas/procedimientos deben ser comunicadas a los empleados y partes externas interesadas. La necesidad de normas internas de seguridad de la información varía dependiendo de las organizaciones.

Cuando algunas de las normas o políticas de seguridad de la información se distribuyen fuera de la organización, se deberá **tener cuidado de no revelar información confidencial**. Algunas organizaciones utilizan otros términos para estos documentos de política, como: normas, directrices o reglas.

Todas estas políticas deben servir de apoyo para la identificación de riesgos mediante la disposición de controles en relación a un punto de referencia que pueda ser utilizado para identificar las deficiencias en el diseño e implementación de los sistemas, y el tratamiento de los riesgos mediante la posible identificación de tratamientos adecuados para las vulnerabilidades y amenazas localizadas.

Esta identificación y tratamiento de los riesgos forman parte de los procesos definidos en la sección de Principios dentro de la política de seguridad o, como se referencia en el ejemplo, suelen formar parte de la propia política del SGSI, tal y como se observa a continuación.

Política de SGSI

En vista de la importancia para el **correcto desarrollo de los procesos de negocio**, los sistemas de información deben estar protegidos adecuadamente.

Una protección fiable permite a la organización percibir mejor sus intereses y llevar a cabo eficientemente sus obligaciones en seguridad de la información. **La inadecuada protección afecta al rendimiento general de una empresa** y puede afectar negativamente a la imagen, reputación y confianza de los clientes, pero, también, de los inversores que depositan su confianza, para el crecimiento estratégico de nuestras actividades a nivel internacional.

El objetivo de la seguridad de la información es asegurar la continuidad del negocio en la organización y reducir al mínimo el riesgo de daño mediante la prevención de incidentes de seguridad, así como reducir su impacto potencial cuando sea inevitable.

Para lograr este objetivo, **la organización ha desarrollado una metodología de gestión del riesgo que permite analizar regularmente el grado de exposición de nuestros activos importantes** frente a aquellas amenazas que puedan aprovechar ciertas vulnerabilidades e introduzcan impactos adversos a las actividades de nuestro personal o a los procesos importantes de nuestra organización.

El éxito en el uso de esta metodología parte de la propia experiencia y aportación de todos los empleados en materia de seguridad, y mediante la comunicación de cualquier consideración relevante a sus responsables directos en las reuniones semestrales establecidas por parte de la dirección, con el objeto de localizar posibles cambios en los niveles de protección y evaluar las opciones más eficaces en coste/beneficio de gestión del riesgo en cada momento, y según el caso.

Los principios presentados en la política de seguridad que acompaña a esta política fueron desarrollados por el grupo de gestión de la información de seguridad con el fin de **garantizar que las futuras decisiones se basen en preservar la confidencialidad, integridad y disponibilidad de la información relevante de la organización**. La organización cuenta con la colaboración de todos los empleados en la aplicación de las políticas y directivas de seguridad propuestas.

El uso diario de los ordenadores por el personal determina el cumplimiento de las exigencias de estos principios y un proceso de inspección para confirmar que se respetan y cumplen por parte de toda la organización. Adicionalmente a esta política, y a la política de seguridad de la organización, se disponen de políticas específicas para las diferentes actividades.

Todas las políticas de seguridad vigentes permanecerán disponibles en la intranet de la organización y se actualizarán regularmente. El acceso es directo desde todas las estaciones de trabajo conectadas a la red de la organización y mediante un clic de ratón desde la página Web principal en el apartado Seguridad de la Información. El objetivo de la política es **proteger los activos de información de la organización en contra de todas las amenazas y vulnerabilidades internas y externas**, tanto si se producen de manera deliberada como accidental.

La dirección ejecutiva de la empresa es la responsable de aprobar una política de seguridad de la información que asegure que:

1. La información estará protegida contra cualquier acceso no autorizado.
2. La confidencialidad de la información, especialmente aquella relacionada con los datos de carácter personal de los empleados y clientes.
3. La integridad de la información se mantendrá en relación a la clasificación de la información (especialmente la de "uso interno").
4. La disponibilidad de la información cumple con los tiempos relevantes para el desarrollo de los procesos críticos de negocio.
5. Se cumplen con los requisitos de las legislaciones y reglamentaciones vigentes, especialmente con la Ley de Protección de Datos y de Firma Electrónica.
6. Los planes de continuidad de negocio serán mantenidos, probados y actualizados al menos con carácter anual.
7. La capacitación en materia de seguridad se cumple y se actualiza suficientemente para todos los empleados.
8. Todos los eventos que tengan relación con la seguridad de la información, reales como supuestos, se comunicarán al responsable de seguridad y serán investigados.

Adicionalmente, se dispone de **procedimientos de apoyo** que incluyen el modo específico en que se deben acometer las directrices generales indicadas en las políticas y por parte de los responsables designados.

El cumplimiento de esta política, así como de la política de seguridad de la información y de cualquier procedimiento o documentación incluida dentro del repositorio de documentación del SGSI, **es obligatorio y atañe a todo el personal de la organización**.

Las visitas y personal externo que accedan a nuestras instalaciones no están exentas del cumplimiento de las obligaciones indiciadas en la documentación del SGSI, y el personal interno observará su cumplimiento.

En cualquier caso, de duda, aclaración o para más información sobre el uso de esta política y la aplicación de su contenido, por favor, consulte por teléfono o e-mail al responsable del SGSI designado formalmente en el organigrama corporativo.

Firmado Sr./Sra. xxxxxxx, Director ejecutivo.