DECLARACIÓN DE LA NORMATIVA DE LA SEGURIDAD DE LA INFORMACIÓN

El presente documento tiene por objeto establecer la política de seguridad de la información para BAYPORT G. S. en base a los requisitos dispuestos en el estándar de seguridad de la información UNE – ISO/IEC 27001:2013, asegurando así la confidencialidad, integridad y disponibilidad de los sistemas de información de

BAYPORT G. S. y por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables.

ALCANCE

El alcance de esta política se circunscribe al alcance establecido para el SGSI definido en el documento BAYPORT G. S.

PLANIFICACIÓN

Las actuaciones a llevar a cabo para cumplir con la declaración de la política de seguridad pasan por la implantación, operación y mantenimiento de un SGSI, que en todo momento está alineado con esta política.

En la fase de planificación se incluye como punto fundamental un estudio de la seguridad de la compañía a través de un análisis de riesgos y el establecimiento de su correspondiente plan de tratamiento de riesgos no aceptados por la organización.

IMPLANTACIÓN

La implantación del SGSI es responsabilidad principal del responsable de seguridad (o responsable del SGSI) apoyado en todo momento por personal técnico y con el total apoyo de gerencia.

En base a los resultados obtenidos en la fase de planificación se implantan determinados controles de seguridad, además de operar los procedimientos del SGSI para dar cumplimiento a las exigencias del estándar ISO 27001.

REVISIÓN

La política de seguridad de la información y el SGSI son revisados regularmente a intervalos planificados o si ocurren cambios significativos para asegurar la continua idoneidad, eficacia y efectividad de la misma. De forma genérica son revisados anualmente junto con los procesos de auditoría interna del SGSI.

Existen procedimientos de monitorización que aportan información sobre el correcto desempeño del SGSI.

La dirección también juega un importante papel en la revisión del sistema, realizando un profundo análisis del sistema y encontrando posibles mejoras y deficiencias.

Con todos estos datos de entrada, se realiza una revisión global por parte del comité de seguridad.

MEJORA

Las posibles mejoras de la política de seguridad de la información y del SGSI son establecidas bien durante las fases de revisión o bien en base a aportaciones que se consideren interesantes tanto de personal de BAYPORT G. S. como de personal externo.

Dichas mejoras son evaluadas y una vez estudiada su viabilidad, son implementadas, operadas y mantenidas.

Todo el SGSI se enmarca dentro del ciclo de Demming (ciclo PDCA), basado en la planificación de actividades, su implantación y operación, su revisión y su posterior mejora. Todo ello aplicado a la seguridad de la información.

RESPONSABILIDADES ASOCIADAS A LOS ACTIVOS

Equipos informáticos y de comunicaciones y sus programas de software

Los usuarios de los sistemas informáticos de BAYPORT G. S. deben esforzarse en hacer y promover un uso eficiente de los mismos a fin de evitar tráfico innecesario en la red e interferencias con su trabajo o el de otros usuarios o con otras redes asociadas ni con los servicios que éstas ofrecen.

El uso de los sistemas de BAYPORT G. S. quedará reservado para las actividades propias a desempeñar en su puesto de trabajo.

Se promoverá el uso responsable de la red interna de la organización.

Será responsabilidad de los propios usuarios la correcta custodia de los activos que tengan en posesión para el desempeño de sus labores contractuales.

Protección del conocimiento

No podrán divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral con BAYPORT G. S. tanto en soporte material como electrónico. Todos los compromisos anteriores deben mantenerse, incluso después de extinguida la relación laboral con la organización.

Propietarios de la información

El propietario de la información será la gerencia de BAYPORT G. S. o un delegado que haya sido nombrado para tal efecto. Sin embargo, será responsabilidad de los usuarios el correcto tratamiento, almacenamiento y no divulgación de la información a la que tengan acceso como consecuencia del desempeño de sus actividades laborales

SEGURIDAD DE LA GESTIÓN DE RECURSOS HUMANOS

Se asegurará que todos los empleados, contratistas y los terceros entienden sus responsabilidades y son adecuados para llevar a cabo las funciones que les corresponden, así como para reducir el riesgo de robo, fraude o de uso indebido de los recursos puestos a su disposición.

Se asegurará que todos los empleados, contratistas y los terceros son conscientes de las amenazas y problemas que afectan a la seguridad de la información y de sus responsabilidades y obligaciones, y de que están preparados para cumplir la política de seguridad de la organización en el desarrollo habitual de su trabajo, y para reducir el riesgo de error humano.

Se asegurará que todos los empleados, contratistas y los terceros abandonan la organización o cambian de puesto de trabajo de forma ordenada y sin comprometer la seguridad de la misma.

SEGURIDAD FÍSICA Y DEL ENTORNO

Se prevendrá todo tipo de acceso físico no autorizado, daños o intromisiones en las instalaciones y en la información de BAYPORT G. S.

Se tomarán las medidas de seguridad necesarias para evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos o que puedan provocar la interrupción de las actividades de BAYPORT G. S..

No se dejarán puestas llaves en puertas, armarios o cajones ni se dejarán puertas o ventanas abiertas cuando no haya nadie en la oficina.

Los portátiles serán llevados en todo momento con la persona asignada al uso del mismo, no dejándolos bajo ningún concepto en la oficina cuando dicha persona se ausente de la misma y esta quede vacía.

En caso de realizar teletrabajo, el empleado se asegurará de disponer de un entorno de trabajo adecuado y proteger los sistemas de los que es responsable.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

Los usuarios de Internet deben esforzarse en hacer y promover un uso eficiente de las redes a fin de evitar tráfico innecesario en la red e interferencias con el trabajo de otros usuarios o con otras redes asociadas ni con los servicios que éstas ofrecen

El uso del sistema informático de BAYPORT G. S. para acceder a redes privadas o públicas, se limitará a los temas directamente relacionados con la actividad y los cometidos del puesto de trabajo del usuario.

Se hará un uso responsable del correo electrónico así como de la información transmitida a través de este medio, preservando su confidencialidad e integridad. Todos los mails mandados a más de un destinatario serán enviados con copia oculta y se solicitará el acuse de recibo que provea el gestor de correo.

Cualquier fichero introducido en la red o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus o cualquier tipo de código malicioso.

Cualquier soporte informático con datos de carácter personal recibido deberá ser registrado, siguiendo el procedimiento establecido. Dicho registro será realizado exclusivamente por el Responsable de Seguridad de la Información o persona en quien delegue. Los soportes que contengan información de carácter personal tendrán una parte cifrada en la que se almacenarán dichos datos.

Está permitido utilizar la información a la que tenga acceso en BAYPORT G. S. únicamente en la forma exigida por el desempeño de sus funciones en la organización y no puede disponer de ella de ninguna otra forma o para otra finalidad diferente.

Se prohíben expresamente las siguientes actividades:

- No está permitido instalar "motu propio" ningún producto informático en el sistema de información de BAYPORT G. S. Todas aquellas aplicaciones necesarias para el desempeño de su trabajo serán instaladas únicamente por personal debidamente autorizado de la organización o empresa prestataria de los servicios informáticos.
- Intentar distorsionar o falsear los registros LOG del sistema.
- Extraer información por medios extraíbles o de cualquier otra forma, sin la autorización expresa de La Dirección.
- Comunicar y enviar información no relacionado con el desarrollo diario del trabajo sin la autorización expresa de La Dirección.
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. (Esta actividad puede constituir un delito de interceptación de las telecomunicaciones, previsto en el artículo 197 del Código Penal).
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos.
- Intentar aumentar el nivel de privilegios de un usuario en el sistema.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de BAYPORT G. S. o de terceros. (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal).
- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.

- Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento de BAYPORT G. S..
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por BAYPORT G. S., o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
- Instalar copias ilegales de cualquier programa, incluidos los corporativos.
- Borrar cualquiera de los programas instalados legalmente sin autorización de BAYPORT G. S..
- Utilizar los recursos telemáticos, incluido el acceso a la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.
- En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado entre en posesión de información confidencial bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le irrogue derecho alguno de posesión, o titularidad o copia sobre la referida información. Asimismo, el trabajador deberá devolver dichos materiales a BAYPORT G. S. inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación laboral. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento de la empresa, no supondrá, en ningún caso, una modificación de esta cláusula. El incumplimiento de esta obligación puede constituir un delito de revelación de secretos, previsto en el artículo 197 y siguientes del Código Penal y dará derecho a BAYPORT G. S. a exigir al usuario una indemnización económica. Asimismo, se recuerda que el trabajador será responsable frente a la organización y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a la compañía las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para las finalidades propias de la empresa, en la red corporativa del mismo.

- Enviar o reenviar mensajes en cadena o de tipo piramidal

BAYPORT G. S. se reserva el derecho de revisar, con previo aviso, los mensajes de correo electrónico de los usuarios de la red y los archivos LOG del servidor, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la organización como responsable civil subsidiario.

La documentación en soporte papel deberá ser guardada y custodiada en sus archivos correspondientes.

Cuando concluya la jornada laboral, el usuario deberá evitar dejar documentación encima de las mesas o fuera de sus lugares de archivo, que deberán permanecer cerrados con llave.

Respecto a la documentación que se imprima, el usuario será responsable de su recogida, que deberá efectuarse con carácter inmediato, evitando el acceso a la documentación por usuarios no autorizados.

La documentación que no sea de utilidad para el usuario, deberá ser destruida utilizando para ello las destructoras de papel existentes.

CONTROL DE ACCESOS

Se controlará el acceso a los sistemas de información de BAYPORT G. S. para que solo sea realizado por personal autorizado y en las condiciones de seguridad que la organización ha decido operar.

Se asegurará el acceso de un usuario autorizado y se prevendrá el acceso de usuarios no autorizados a los sistemas de información de BAYPORT G. S..

IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

Se prevendrá el acceso no autorizado a los servicios de red para los usuarios que no hayan sido legitimados.

Se usarán métodos seguros de autenticación para conexiones externas por parte de usuario autorizados.

Los grupos de servicios de información, usuarios y sistemas de información deberán estar segregados en la red.

La información transmitida a través de redes de telecomunicaciones se hará de forma segura.

Con relación a las contraseñas se habrán de observar las siguientes normas:

- La contraseña de acceso al sistema caducará a los 180 días.

- El usuario será el encargado de modificarla en el momento de realizar el primer acceso al sistema, ya que se le solicitara automáticamente, caso contrario, será el usuario el encargado de realizar dicho cambio.

- Se evitarán nombres comunes, números de matriculas de vehículos, teléfonos, nombres de familiares, amigos, etc. y derivados del nombre de usuario como permutaciones o cambio de orden de las letras, transposiciones, repeticiones de un único carácter, etc.
- Las contraseñas usadas en cualquier sistema o servicio serán como mínimo de 8 caracteres, combinando letra y números.
- No se accederá al sistema utilizando el identificador y la contraseña de otro usuario. Las responsabilidades de cualquier acceso realizado utilizando un identificador determinado, recaerán sobre el usuario al que hubiera sido asignado.
- Se debe bloquear el equipo cuando no vaya a ser usado, o usar mecanismos automáticos, no dejándolo nunca desatendido.
- Se seguirá una política de puesto de trabajo despejado y mesas limpias, no dejando información confidencial o privada a la vista.
- Si se sospecha que la contraseña es conocida por otros usuarios, se procederá a informar al administrador de sistemas para su revocación y sustitución por una nueva.

Se prohíben expresamente las siguientes actividades:

- Compartir o facilitar el identificador de usuario y la contraseña para acceder a los sistemas de información a otra persona física, incluido el personal de BAYPORT G. S.. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física que utilice de forma no autorizada el identificador del usuario.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad.

Acceso a Internet

- El uso del sistema informático de BAYPORT G. S. para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad de la compañía y los cometidos del puesto de trabajo del usuario.

- El acceso a debates en tiempo real (Chat / IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido.
- El acceso a páginas web (WWW), grupos de noticias (Newsgroups) y otras utilidades como FTP, telnet, etc. se limita a aquéllos que contengan información relacionada con la actividad de BAYPORT G. S. o con los cometidos del puesto de trabajo del usuario.
- BAYPORT G. S. se reserva el derecho de comprobar, de forma aleatoria y con previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa con el fin de prevenir un uso fraudulento, ilegal, abusivo o no autorizado de Internet. Dicha comprobación incluye la revisión de registros que muestran los ficheros cargados, los que se han accedido, las páginas web visitadas y los usuarios que han ejecutado tales acciones así como el momento en el que se han producido.
- Cualquier persona que acceda a Internet a través de la red de BAYPORT G. S. acepta esta comprobación así como las normas aquí establecidas, asumiendo la imposición de acciones disciplinarias por incumplimiento de las citadas normas.
- Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.
- Se prohíbe la descarga a través de Internet de software de origen desconocido o de propiedad del usuario en los sistemas de BAYPORT G. S., salvo que exista una autorización previa.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La política de seguridad relativa a la adquisición, desarrollo y mantenimiento de sistemas consta de las siguientes partes:

- Contemplar requisitos de seguridad en las fases de análisis y diseño de sistemas de información.
- Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas.
- Separar los entornos de prueba y producción.
- Avisar al administrador de sistemas cuando haya cambios importantes en los sistemas para el correcto desempeño de las copias de seguridad.

Protección de los sistemas operativos y otras unidades

Se prevendrá el acceso no autorizado a los sistemas operativos, así como su actualización para corregir vulnerabilidades detectadas y se proveerán de las medidas técnicas de seguridad oportunas.

Estará restringido y controlado el uso de aplicaciones no autorizadas que puedan invalidar las medidas de seguridad implantadas.

GESTIÓN DE INCIDENCIAS

Toda incidencia en materia de seguridad deberá comunicarse, siguiendo el procedimiento establecido. Dicha notificación será realizada a través de correo electrónico a rrhh@baypor.eu y mac@bayport.eu . Una vez recibida el Responsable de Seguridad será el encargado de darle seguimiento, completar las notificaciones establecidas en el procedimiento correspondiente, establecer las acciones para su corrección y comunicar al usuario la resolución o estado de la misma.

CONTINUIDAD DEL NEGOCIO

Todos los empleados colaborarán en la oportuna reanudación de todos los servicios críticos para BAYPORT G. S. en caso de una contingencia grave, ayudando de estar forma a que se restablezcan la mayoría de los servicios en el mínimo tiempo posible.

CUMPLIMIENTO LEGAL

Se evitará cualquier tipo de incumplimiento de las leyes u obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad que afecten a los sistemas de información de BAYPORT G. S..

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial.

En cumplimiento de lo establecido en el artículo 5 de la ley orgánica de protección de datos (LOPD) se informa al empleado de lo siguiente:

Que los datos del contrato de trabajo del trabajador se incorporan al fichero <<RRHH>> perteneciente a BAYPORT G. S. con domicilio en Polígono Industrial Tres Caminos Calle La Dorada, s/n 11510 Puerto Real – Cádiz y que tal fichero tiene como finalidad mantener la relación contractual establecida y la elaboración de la contabilidad de la sociedad.

1. Que la negativa a facilitar los datos pedidos implica no poder realizar su contratación de acuerdo con la legislación vigente, pues son necesarios para la creación y mantenimiento de la relación contractual.

Que tiene derecho de acceso, rectificación, cancelación y oposición a sus datos personales que constan en el fichero anterior, debiendo dirigirse para ejercitarlo a BAYPORT G. S., Polígono Industrial Tres Caminos Calle La Dorada, s/n 11510 Puerto Real – Cádiz o a la siguiente dirección de correo rrhh@bayport.eu.

1. Que sus datos van a ser comunicados, DENTRO DEL MARCO LEGAL, a los correspondientes organismos administrativos, de trabajo y seguridad social.

2. Que sus datos personales recogidos en el fichero descrito son cedidos a la gestoría de la empresa con la finalidad Gestión de nóminas.

En el caso de producirse cambios en sus datos se ruega que sea comunicado con el fin de mantener los datos actualizados.

Fdo:

Miguel Angel Criado

Director General