Normativa para la gestión segura de la información para proveedores

1. Objeto:

El objeto de este documento es establecer el marco normativo en relación con la seguridad de la información para las organizaciones proveedoras de la Organización que acceden a su información, sistemas de información o recursos, con el fin de proteger su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Para ello, las organizaciones proveedoras se responsabilizan de informar a sus personas empleadas y subcontratistas que prestan servicio a la Organización.

2. Alcance

Todas las actividades desarrolladas para la Organización por organizaciones proveedoras que acceden a su información, sistemas de información o recursos.

El apartado "3. Directrices generales" es aplicable a cualquier organización proveedora, independientemente del tipo de servicio prestado.

El apartado "4. Directrices específicas" es aplicable exclusivamente a aquellas organizaciones proveedoras cuyos servicios proporcionados se correspondan con el tipo de servicio indicado en cada caso, tal y como se indica al comienzo del citado apartado.

3. Directrices generales

3.1. Prestación del servicio

Las organizaciones proveedoras sólo podrán desarrollar para la Organización aquellas actividades cubiertas bajo el correspondiente contrato de prestación de servicios.

De acuerdo con lo establecido en las cláusulas asociadas al contrato de prestación de servicios, todas las personas externas que desarrollen labores para la Organización deberán cumplir las normas de seguridad recogidas en el presente documento. En caso de incumplimiento de cualquiera de estas obligaciones, la Organización se reserva el derecho de veto a la persona que haya cometido la infracción, así como la adopción de las medidas sancionadoras que se consideren pertinentes en relación con la organización proveedora.

La organización proveedora deberá asegurar que todas sus personas tienen la capacitación apropiada para el desarrollo del servicio prestado.

Cualquier tipo de intercambio de información que se produzca entre la Organización y la organización proveedora se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios correspondiente, de modo que dicha información no podrá ser utilizada fuera de dicho marco ni para otros fines.

Los departamentos de operaciones y producto centralizan los esfuerzos globales de protección de los activos de la Organización.

De forma genérica, los activos incluyen:

- La información protegida, es decir, aquella información que permite identificar a personas físicas y/o jurídicas, y aquella relativa a la configuración de los sistemas de información y las redes de comunicaciones.
- Los asociados para el tratamiento de la información protegida (software, hardware, redes de comunicaciones, soportes de información, equipamiento auxiliar e instalaciones).

3.2. Confidencialidad de la información

Las personas externas que tenga acceso a información de la Organización deberán considerar que dicha información, por defecto, tiene el carácter de protegida. Sólo se podrá considerar como información no protegida aquella información a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por la Organización

Se evitará la revelación, modificación, destrucción o mal uso de la información cualquiera que sea el soporte en el que se encuentre.

Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior información protegida, salvo que esté debidamente autorizado.

Se minimizará el número de informes en formato papel que contengan información protegida y se mantendrán los mismos en lugar seguro y fuera del alcance de terceras personas.

En el caso de que, por motivos directamente relacionados con el puesto de trabajo, la persona empleada de la organización proveedora entre en posesión de información protegida contenida en cualquier tipo de soporte, deberá entender que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información. Asimismo, la persona empleada deberá devolver el o los soportes mencionados, 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 con la Organización de su empresa.

Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que las personas externas desarrollen para la Organización

El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos.

Para garantizar la seguridad de los datos de carácter personal, las personas de la organización proveedora deberán observar las siguientes normas de actuación, además de las consideraciones ya mencionadas:

- Solo podrán crear ficheros cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán guardados en unidades locales de disco de los puestos PC de las personas usuarias y deberán ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.
- No se albergarán datos de carácter personal en las unidades locales de disco de los puestos PC de persona usuaria.
- La salida de soportes y documentos (envío de e-mails incluido), fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por la Organización y se realizará según el procedimiento definido.
- Los soportes y documentos deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido a las personas autorizadas.
- La transmisión de datos de carácter personal especialmente protegidos (p.e. Salud), a través de redes de telecomunicaciones (p.e. Correo electrónico) se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceras personas.

3.3. Propiedad intelectual

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por la normativa de propiedad intelectual.

Las personas usuarias únicamente podrán utilizar material autorizado por la Organización para el desarrollo de sus funciones.

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los sistemas de información de la Organización.

Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización por escrito.

la Organización únicamente autorizará el uso de material producido por él mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

3.4. Intercambio de información

Ninguna persona deberá ocultar o manipular su identidad en ninguna circunstancia.

La distribución de información ya sea en formato electrónico o físico se realizará mediante los recursos determinados en el contrato de prestación de servicios para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato. la Organización se reserva, en función del riesgo identificado, la implantación de medidas de control, registro y auditoría sobre estos recursos de difusión.

En relación con el intercambio de información dentro del marco del contrato de prestación de servicios, se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por los derechos de autor infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transferencia de información protegida a terceras partes no autorizadas.
- Transmisión o recepción de aplicaciones no relacionadas con el negocio.
- Participación en actividades de Internet, como grupos de noticias, juegos u otras que no estén directamente relacionadas con la prestación del servicio.

Todas las actividades que puedan dañar la imagen y reputación de la Organización están prohibidas en Internet y en cualquier otro lugar.

3.5. Uso apropiado de los recursos

La organización proveedora se compromete a informar periódicamente a la Organización de los activos con los que proporciona el servicio.

La organización proveedora se compromete a utilizar los recursos dispuestos para la prestación del servicio de acuerdo con las condiciones para las que fueron diseñados e implantados.

Los recursos que la Organización pone a disposición de las personas externas, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron proporcionados. la Organización se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

Todos los equipos de la organización proveedora que se conecten a la red de producción de la Organización serán de las marcas y modelos homologados. La organización proveedora pondrá a disposición de la Organización dichos equipos para que éste coordine la instalación del software homologado y los configure apropiadamente.

Cualquier fichero introducido en la red de la Organización o en cualquier equipo conectado a ella a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal, y control de malware.

Se deberán restituir a la Organización todos los activos, sin retraso injustificado, después de la finalización del contrato. Todos los ordenadores personales a los que la Organización les haya instalado software se llevarán a la Organización para que se formatee el disco duro a la finalización del servicio.

Se prohíbe expresamente:

- El uso de los recursos proporcionados por la Organización para actividades no relacionadas con el propósito del servicio.
- La conexión a la red de producción de la Organización de equipos y/o aplicaciones que no estén especificados como parte del software o de los estándares de los recursos informáticos propios.
- Introducir en los sistemas de información o la red corporativa de la Organización contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente en la red corporativa de la Organización cualquier tipo de malware (virus, gusanos, troyanos, programas espía, ransomware, ...), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. Todas las personas con acceso a la red de la Organización tendrán la obligación de utilizar programas antimalware actualizados.
- Obtener sin autorización explícita otros derechos o accesos distintos a aquellos que la Organización les haya asignado.
- Acceder sin autorización explícita a áreas restringidas de los sistemas de información de la Organización
- Distorsionar o falsear los registros “log” de los sistemas de información de la Organización
- Descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la Organización
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otras personas usuarias, ni dañar o alterar los recursos informáticos de la Organización
- Destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos con información protegida (estos actos pueden constituir un delito).
- Albergar información protegida en las unidades locales de disco de los puestos PC de persona usuaria.

3.6. Responsabilidades de la persona usuaria

Las organizaciones proveedoras de servicios deberán asegurarse de que todas las personas que desarrollan labores para la Organización respeten los siguientes principios básicos dentro de su actividad:

- Cada persona con acceso a información de la Organización es responsable de la actividad desarrollada por su identificador de persona usuaria y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de persona usuaria, garantizando que la clave asociada sea

únicamente conocida por la propia persona usuaria, no debiendo revelarse al resto de las personas bajo ningún concepto.

- Las personas usuarias no deberán utilizar ningún identificador de otra persona usuaria, aunque dispongan de la autorización del propietario.
- Las personas usuarias conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.
- Cualquier persona con acceso a la información protegida deberá seguir las siguientes directivas en relación con la gestión de las contraseñas:
- Seleccionar contraseñas de calidad, es decir, difícilmente adivinables por el resto de las personas usuarias.
- Pedir el cambio de la contraseña siempre que exista un posible indicio de conocimiento por parte de otras personas usuarias.
- Cambiar las contraseñas como mínimo una vez cada 90 días y evitar la reutilización de antiguas contraseñas.
- Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión ("login").
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión (p.e. Aquellas almacenadas en navegadores).
- Notificar cualquier incidente de seguridad relacionada con sus contraseñas como pérdida, robo o indicio de pérdida de confidencialidad.
- Cualquier persona con acceso a la información protegida deberá velar por que los equipos queden protegidos cuando vayan a quedar desatendidos.
- Cualquier persona con acceso a información protegida deberá respetar al menos las siguientes normas de escritorio limpio, con el fin de proteger los documentos en papel, soportes informáticos y dispositivos portátiles de almacenamiento y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:
- Almacenar bajo llave los documentos en papel y los medios informáticos, cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Bloquear las sesiones de persona usuaria o apagar el PC al dejarlo desatendido.
- Proteger tanto los puntos de recepción y envío de información (correo postal, máquinas de scanner y fax) como los equipos de duplicado (fotocopiadora, fax y scanner). La reproducción o envío de información con este tipo de dispositivos quedará bajo la responsabilidad de la persona usuaria.
- Retirar, sin retraso injustificado, cualquier información protegida una vez impresa.
- Destruir la información protegida una vez no sea necesaria.
- Las personas con acceso a sistemas y/o información de la Organización nunca deberán, sin autorización por escrito, realizar pruebas para detectar y/o explotar una supuesta debilidad, evento o incidente de seguridad.
- Ninguna persona con acceso a sistemas y/o información de la Organización intentará sin autorización expresa y por escrito por ningún medio transgredir el sistema de seguridad y las autorizaciones. Se prohíbe la captura de tráfico de red por parte de las personas usuarias, salvo que se estén llevando a cabo tareas de auditoría autorizadas por escrito.
- Todas las personas que accedan a la información protegida deberán seguir las siguientes normas de actuación:
- Proteger la información protegida de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
- Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
- Contar con la autorización necesaria para obtener el acceso a los sistemas de información y/o la información.

3.7. Equipo de persona usuaria

Las organizaciones proveedoras de servicios deberán asegurarse de que todo el equipamiento informático de persona usuaria utilizado para acceder a información protegida cumple las siguientes normas:

Ante la inactividad de la persona usuaria, el equipo deberá bloquearse automáticamente en un plazo máximo de 15 minutos.

Ningún equipo de persona usuaria dispondrá de herramientas que puedan transgredir los sistemas de seguridad y las autorizaciones.

- Los equipos de persona usuaria se mantendrán de acuerdo con las especificaciones del fabricante.
- Todos los equipos de persona usuaria estarán adecuadamente protegidos frente a malware:
    - El software antimalware se deberá instalar y usar en todos los ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
    - Se mantendrán al día con las últimas actualizaciones de seguridad disponibles.
    - El software antimalware deberá estar siempre habilitado y actualizado.
- Se velará especialmente por la seguridad de todos los equipos móviles de persona usuaria que contengan información protegida o permitan acceder a ella de algún modo:
- Verificando que no incluyen más información que la que sea estrictamente necesaria.
- Garantizando que se aplican controles de acceso a dicha información.
- Minimizando los accesos a dicha información en presencia de personas ajenas al servicio prestado.
- Transportando los equipos en fundas, maletines o equipamiento similar que incorpore la apropiada protección frente a agentes ambientales.

3.8. Gestión del equipamiento hardware

Las organizaciones proveedoras de servicios deberán asegurarse de que todos los equipos proporcionados por la Organización para la prestación de servicios, independientemente del tipo que sean, se gestionan apropiadamente. Para ello deberán cumplir las siguientes normas:

- La organización proveedora deberá mantener una relación actualizada de equipos proporcionados por la Organización y personas usuarias de dichos activos, o personas responsables asociadas en caso de que los activos no sean de uso unipersonal. Dicha relación podrá ser requerida por la Organización.
- Siempre que una organización proveedora quiera reasignar algún equipo de la Organización que haya contenido información protegida deberá devolverlo temporalmente para que se puedan llevar a cabo los procedimientos de borrado seguro necesarios de forma previa a su reasignación.
- En caso de que una organización proveedora quiera dar de baja de la relación de equipos de la Organización recibidos alguno de ellos, siempre deberá devolverlos, para que la Organización pueda tratar dicha baja de forma apropiada.
- En caso de que una organización proveedora cese en la prestación del servicio, deberá devolver a la Organización toda la relación de equipos recibidos, tal y como establecen los correspondientes contratos de prestación de servicios. Sólo en el caso de documentos en papel y soportes informáticos la organización proveedora podrá proceder a su eliminación segura, en cuyo caso deberá notificar a la Organización dicha eliminación.

4. Directrices especificas

4.1. Ámbito de aplicación

Todas las organizaciones proveedoras deberán cumplir, además de las normas generales, las específicas recogidas en el presente apartado que les correspondan en cada caso, en función de las características del servicio prestado a la Organización.

Las tipologías de servicio que se contemplan son las que se indican a continuación.

- Lugar de ejecución del servicio: En función del lugar principal en el que se desarrollen los servicios se distinguen dos casos:
  - la Organización: La organización proveedora presta el servicio principalmente desde la propia sede de la Organización.
  - Remoto: La organización proveedora presta el servicio principalmente desde sus propias dependencias, pese a que se puedan llevar a cabo actividades puntuales en la sede de la Organización.
- Propiedad de las infraestructuras TIC utilizadas: En función de quién sea el propietario de las principales infraestructuras TIC (comunicaciones, equipos de persona usuaria, software) utilizadas para prestar el servicio se distinguen dos casos:
  - la Organización.
  - Organización proveedora.
- Nivel de acceso a los sistemas de la Organización: En función del nivel de acceso a los sistemas de información de la Organización se distinguen tres casos:
  - Con acceso privilegiado: El servicio prestado requiere del acceso privilegiado a los sistemas de información de la Organización, con capacidad para administrar dichos sistemas y/o los datos de producción que procesan.
  - Con acceso de nivel de persona usuaria: El servicio prestado requiere de la utilización de los sistemas de información de la Organización, de modo que las personas que prestan el servicio disponen de cuentas de persona usuaria que les permiten acceder a alguno de dichos sistemas con privilegios habituales.
  - Sin acceso: El servicio prestado no requiere de la utilización de los sistemas de información de la Organización, de modo que las personas que prestan el servicio no disponen de cuentas de persona usuaria en dichos sistemas.

En función de cada una de las tres categorías en las que se encuadre cada servicio, la organización proveedora deberá cumplir, adicionalmente a las normas generales de seguridad, las específicas recogidas en los apartados que se indican en la siguiente tabla:

	LUGAR		***INFRAESTRUCTURA***		***ACCESO***		
	La Organización	*Remoto*	*La Organización*	*Organización proveedor*	*Privilegiado*	*Normal*	*Sin acceso*
selección de personas	NO	NO	NO	NO	SÍ	NO	NO
auditoría de seguridad	NO	NO	NO	NO	SÍ	NO	NO
comunicación de incidentes	SÍ	SÍ	SÍ	NO	SÍ	SÍ	NO
seguridad física	NO	SÍ	NO	NO	NO	NO	NO
gestión de activos	NO	NO	NO	SÍ	NO	NO	NO
arquitectura seguridad	NO	NO	NO	SÍ	SÍ	SÍ	NO

	LUGAR		***INFRAESTRUCTURA***		***ACCESO***		
	La Organización	*Remoto*	*La Organización*	*Organización proveedor*	*Privilegiado*	*Normal*	*Sin acceso*
seguridad sistemas	NO	NO	NO	SÍ	NO	NO	NO
seguridad red	NO	NO	NO	SÍ	NO	NO	NO
trazabilidad de uso de los sistemas	NO	NO	NO	SÍ	SÍ	NO	NO
control y gestión de identidades y accesos	NO	NO	NO	SÍ	NO	NO	NO
gestión cambios	NO	NO	NO	SÍ	SÍ	SÍ	NO
gestión técnica de cambios	NO	NO	NO	NO	SÍ	NO	NO
seguridad en desarrollo	NO	NO	NO	NO	SÍ	SÍ	NO
gestión contingencias	NO	NO	NO	SÍ	NO	NO	NO

4.2. Ámbito de aplicación

La organización proveedora deberá verificar los antecedentes profesionales de las personas asignadas al servicio, garantizando a la Organización que en el pasado no ha sido sancionado por mala praxis profesional ni se ha visto envuelto en incidentes relacionadas con la confidencialidad de la información tratada que le hayan supuesto algún tipo de sanción.

La organización proveedora deberá garantizar a la Organización la posibilidad de baja inmediata de las personas asignadas al servicio de cualquier persona en relación con la cual la Organización desee ejercer el derecho de veto, de acuerdo con los condicionantes establecidos en el apartado "3.1. Prestación del servicio".

4.3. Auditoría de seguridad

La organización proveedora deberá permitir que la Organización lleve a cabo las auditorías de seguridad solicitadas, colaborando con el equipo auditor y facilitando todas las evidencias y registros le sean requeridos.

El alcance y profundidad de cada auditoría será establecido expresamente por la Organización en cada caso. Las auditorías se llevarán a cabo siguiendo la planificación que se acuerde en cada caso con la organización proveedora del servicio.

la Organización se reserva el derecho de realizar auditorías extraordinarias adicionales, siempre que se den causas específicas que lo justifiquen.

4.4. Comunicación de incidentes

Cuando detecte cualquier vulnerabilidad, evento y/o incidente de seguridad de la información deberá notificarlo inmediatamente a través del buzón de correo electrónico: seguridadinformacion@ludusglobal.com

Cualquier persona usuaria podrá trasladar a través del citado buzón aquellos eventos, sugerencias, vulnerabilidades, … que puedan tener relación con la seguridad de la información y las directrices contempladas en las presentes normas de las que tenga conocimiento.

Se deberá notificar a través del citado buzón cualquier incidente que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal (p.e. Pérdida de listados y/o soportes informáticos, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos de copias de seguridad, …).

El citado buzón centraliza la recogida, análisis y gestión de los incidentes notificados.

Si no se tuviera acceso al buzón, se deberán utilizar los cauces de comunicación establecidos dentro del propio servicio, de modo que sea el interlocutor de la Organización quien comunique el incidente de seguridad.

4.5. Seguridad física

La sede deberá estar cerrada y deberá contar con algún sistema de control de acceso.

Existirá algún tipo de control de las visitas, al menos en áreas de acceso público y/o de carga y descarga.

La sede deberá contar, al menos, con sistemas adecuados de detección y extinción de incendios, y deberá estar construida de modo que ofrezca una suficiente resistencia frente a inundaciones.

Si se mantiene algún tipo de copia de seguridad, los sistemas que alberguen y/o procesen dicha información deberán estar ubicados en un área especialmente protegida, que incluya al menos las siguientes medidas de seguridad:

- El área especialmente protegida deberá tener un sistema de control de acceso independiente al de la sede.
- Se limitará el acceso a las personas externas a las áreas especialmente protegidas. Este acceso se asignará únicamente cuando sea necesario y se encuentre autorizado, y siempre bajo la vigilancia de personas autorizadas.
- Se mantendrá un registro de todos los accesos de personas ajenas.
- Las personas externas no podrán permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.
- El consumo de alimentos o bebidas en estas áreas especialmente protegidas estará prohibido.
- Los sistemas ubicados en estas áreas deberán contar con algún tipo de protección frente a fallos de alimentación.

4.6. Gestión de activos

La organización proveedora deberá contar con un registro de activos actualizado en el que se puedan identificar los activos utilizados para la prestación del servicio.

Todos los activos utilizados para la prestación del servicio deberán tener una persona responsable, que se deberá asegurar de que dichos activos incorporan las medidas de seguridad mínimas establecidas por la organización proveedora, y que al menos deben ser las especificadas en la presente normativa.

La organización proveedora deberá notificar a la Organización las bajas de los activos utilizados para la prestación del servicio. Si dicho activo contiene otra propiedad de la Organización (hardware, software u otro tipo de activos), deberá ser entregado a la Organización previamente a llevar a cabo la baja para que la Organización proceda a la retirada de los activos de su propiedad.

Siempre que un activo haya contenido información protegida, la organización proveedora deberá llevar a cabo las bajas de activos garantizando la eliminación segura de dicha información, aplicando

funciones de borrado seguro o destruyendo físicamente el activo, para que la información que haya contenido no pueda ser recuperable.

4.7. Arquitectura de seguridad

Siempre que la organización proveedora de servicios realice trabajos de desarrollo y/o pruebas de aplicaciones para la Organización o con información protegida, los entornos con los que se lleven a cabo dichas actividades deberán estar aislados entre sí y también aislados de los entornos de producción en los que se albergue o procese información protegida.

Todos los accesos a los sistemas de información que alberguen o procesen información protegida deberán estar protegidos, al menos, por un cortafuegos, que limite la capacidad de conexión a ellos.

Los sistemas de información que alberguen o procesen información especialmente sensible deberán estar aislados del resto.

4.8. Seguridad de sistemas

Los sistemas de información que alberguen o traten información protegida deberán registrar los eventos más significativos en torno a su funcionamiento. Estos registros de actividad estarán contemplados dentro de la normativa de copias de seguridad de la organización proveedora.

Los relojes de los sistemas de la organización proveedora que procesen o alberguen información protegida estarán sincronizados entre sí y con la hora oficial.

La organización proveedora del servicio garantizará que la capacidad de los sistemas de información que guarden o traten información protegida se gestiona adecuadamente, evitando potenciales paradas o malos funcionamientos de dichos sistemas por saturación de recursos.

Los sistemas de información que alberguen o procesen información protegida estarán adecuadamente protegidos frente a software malicioso, aplicando las siguientes precauciones:

- Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles, en los entornos de desarrollo, prueba y producción.
- El software antimalware se deberá instalar y usar en todos los servidores y ordenadores personales para reducir el riesgo asociado con el software malicioso.
- El software antimalware deberá estar siempre habilitado y actualizado.

La organización proveedora establecerá una normativa de copias de seguridad que garantice la salvaguarda de cualquier dato o información relevante para el servicio prestado, con una periodicidad semanal.

Siempre que se utilice el correo electrónico en relación con el servicio prestado, la organización proveedora deberá respetar las siguientes premisas:

- No se permitirá la transmisión vía correo electrónico de información protegida salvo que la comunicación electrónica esté cifrada y el envío esté autorizado por escrito.
- No se permitirá la transmisión vía correo electrónico de información que contenga datos de carácter personal especialmente protegidos (p.e. Salud), salvo que la comunicación electrónica esté cifrada y el envío esté autorizado por escrito.
- Siempre que para la prestación del servicio se haga uso del correo electrónico de la Organización se deberán respetar, al menos, los siguientes principios:
- Se considerará al correo electrónico como una herramienta más de trabajo proporcionada con el fin exclusivo del servicio contratado. Esta consideración facultará a la Organización a implementar sistemas de control destinados a velar por la protección y el buen uso de este recurso. Esta facultad, no obstante, se ejercerá salvaguardando la dignidad de las personas y su derecho a la intimidad.

- El sistema de correo electrónico de la Organización no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.
- Las personas usuarias no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples personas usuarias).

El acceso a los sistemas de información que alberguen o procesen información protegida deberá realizarse siempre de forma autenticada, al menos mediante la utilización de un identificador de persona y una contraseña asociada.

Los sistemas de información que alberguen o procesen información protegida deberán contar con sistemas de control de acceso que limiten el acceso a dicha información exclusivamente a las personas del servicio.

Las sesiones de acceso a los sistemas de información que alberguen o procesen información protegida deberán bloquearse automáticamente tras un cierto tiempo de inactividad de las personas usuarias.

Siempre que se haga uso de software facilitado por la Organización se deberán atender las siguientes normas:

- Todas las personas que accedan a los sistemas de información de la Organización deberán utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.
- Todas las personas tienen prohibido instalar copias ilegales de cualquier software.
- Se prohíbe el uso de software no validado por la Organización.
- También está prohibido desinstalar cualquiera de los programas instalados por la Organización.

4.9. Seguridad de red

Las redes a través de las que circule la información protegida deberán estar adecuadamente gestionadas y controladas, asegurándose de que no existen accesos no controlados ni conexiones cuyos riesgos no estén apropiadamente gestionados por la organización proveedora.

Los servicios disponibles en las redes a través de las que circule la información protegida deberán limitarse en la medida de lo posible.

Las redes que permitan el acceso a la infraestructura TIC de la Organización deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:

- El acceso de personas usuarias remotos a la red de la Organización estará sujeto al cumplimiento de procedimientos de identificación y autenticación previa, y validación del acceso.
- Estas conexiones se realizarán por tiempo limitado y mediante la utilización de redes privadas virtuales o líneas dedicadas.
- En estas conexiones no se permitirá ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas.
- El acceso a las redes a través de las que circule la información protegida deberá estar limitado.
- Todos los equipos conectados a las redes a través de las que circule la información protegida deberán estar apropiadamente identificados, de modo que los tráficos de red puedan ser identificables.
- El teletrabajo, considerado como el acceso a la red corporativa desde el exterior, se regula mediante la aplicación de la siguiente normativa:
- No se permite la utilización de equipamiento no controlado por la Organización para las actividades de teletrabajo.

- Se establecerán criterios de autorización del teletrabajo en base a las necesidades del puesto de trabajo.
- Se establecerán las medidas necesarias para la conexión segura a la red corporativa.
- Se establecerán sistemas de monitorización y auditoría de seguridad para las conexiones establecidas.
- Se controlará la revocación de derechos de acceso y devolución de equipamiento tras la finalización del periodo de necesidad de este.
- Siempre que se haga uso del acceso a Internet proporcionado por la Organización se deberán respetar, adicionalmente, la siguiente normativa:
- Internet es una herramienta de trabajo. Todas las actividades en Internet deberán estar en relación con tareas y actividades de trabajo. Las personas usuarias no deben buscar o visitar sitios que no sirvan como soporte al objetivo de negocio de la Organización o al cumplimiento de su trabajo diario.
- El acceso a Internet desde la red corporativa se restringirá por medio de dispositivos de control incorporados en la misma. La utilización de otros medios de conexión deberá ser previamente validada y estará sujeta a las anteriores consideraciones sobre el uso de Internet.
- Las personas usuarias no deberán usar el nombre, símbolo, logotipo o símbolos similares al de la Organización en ningún elemento de Internet (correo electrónico, páginas Web, etc.) no justificado por actividades estrictamente laborales.
- Únicamente se permitirá la transferencia de datos de o hacia Internet cuando estén relacionadas con actividades del negocio. La transferencia de ficheros no relativa a estas actividades (p.e. La descarga de programas, ficheros multimedia, …) estará prohibida.

4.10. Seguridad de red

Se registrarán los accesos privilegiados conservándose dichos registros de acuerdo con la normativa de copias de seguridad de la Organización.

Se registrará la actividad de los sistemas utilizados para llevar a cabo dicho acceso privilegiado, conservándose dichos registros de acuerdo con la normativa de copias de seguridad de la Organización.

Los errores y fallos registrados en la actividad de los sistemas se analizarán, adoptándose las medidas necesarias para su subsanación.

4.11. Control y gestión de identidades y accesos

Todas las personas usuarias con acceso a un sistema de información dispondrán de una única autorización de acceso compuesta de identificador de persona usuaria y contraseña.

Las personas usuarias serán responsables de toda actividad relacionada con el uso de su acceso autorizado.

Las personas usuarias no deberán utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Las personas usuarias no deberán revelar bajo ningún concepto su identificador y/o contraseña a otra persona, ni mantenerla por escrito a la vista, ni al alcance de terceras personas.

La longitud mínima de la contraseña deberá ser de 6 caracteres y no deberá contener el nombre, apellidos ni el identificador de la persona usuaria en la misma. Deberá ser cambiada cada 45 días ni repetir al menos las 8 contraseñas anteriores.

Igualmente, deberán tener complejidad y ser difícilmente adivinables, por lo que estarán constituidas por combinación al menos 3 de estas 4 opciones en los primeros 8 caracteres:

- Mayúsculas
- Minúsculas
- Números
- Caracteres especiales

Es recomendable utilizar las siguientes directrices para la selección de contraseñas:

- No usar palabras conocidas, ni palabras que se puedan asociar con uno mismo, por ejemplo, el nombre.
- La contraseña no deberá hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se deberá evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, ...
- La clave debería ser algo prácticamente imposible de adivinar. Pero al mismo tiempo debería ser fácilmente recordada por la persona usuaria. Un buen ejemplo es usar el acrónimo de alguna frase o expresión.
- La organización proveedora deberá garantizar que periódicamente se constata que sólo tienen acceso a la información protegida las personas debidamente autorizadas para ello.
- En aquellos casos en los que además se acceda a los sistemas de información de la Organización se deberán considerar, además, la siguiente normativa:
- Ninguna persona usuaria recibirá un identificador de acceso a los sistemas de la Organización hasta que no acepte por escrito la normativa de seguridad vigente.
- Las personas usuarias tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- En caso de que el sistema no lo solicite automáticamente, la persona usuaria deberá cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- En el caso que el sistema no lo solicite automáticamente, la persona usuaria deberá cambiar su contraseña como mínimo una vez cada 90 días.
- Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- En relación con datos de carácter personal, exclusivamente las personas autorizadas para ello podrán conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por la persona responsable del fichero.
- Si una persona usuaria tiene sospechas de que su acceso autorizado (identificador de persona usuaria y contraseña) está siendo utilizado por otra persona, deberá proceder al cambio de su contraseña y notificar el incidente en el buzón de correo electrónico seguridadinformacion@ludusglobal.com .

4.12. Gestión de cambios

Todos los cambios en la infraestructura TIC deberán estar controlados y autorizados, garantizándose que no forma parte de ella componentes no controlados.

Se deberá verificar que todos los nuevos componentes introducidos en la infraestructura TIC de la organización proveedora utilizada para la prestación del servicio funcionan adecuadamente y cumplen los propósitos para los que fueron incorporados.

4.13. Gestión técnica de cambios

Todos los cambios que se lleven a cabo se deberán realizar siguiendo un procedimiento formalmente establecido y documentado, que garantice que se siguen los pasos apropiados para realizar el cambio.

El procedimiento de gestión de cambios deberá garantizar que se minimizan los cambios sobre la infraestructura TIC, limitándose a los estrictamente imprescindibles.

Se deberán probar todos los cambios antes de su despliegue en el entorno de producción, para comprobar que no se producen efectos adversos colaterales o no previstos sobre el funcionamiento y seguridad de la infraestructura TIC.

Las organizaciones proveedoras deberán escanear y mitigar las vulnerabilidades técnicas que presenten las infraestructuras utilizadas para la prestación del servicio, informando a la Organización de todas aquellas asociadas a los componentes críticos.

4.14. Seguridad en desarrollo

Todo el proceso de desarrollo de software externalizado será controlado y supervisado por la Organización

Se incorporarán mecanismos de identificación, autentificación, control de acceso, auditoría e integridad en todo el ciclo de vida de diseño, desarrollo, implantación y operación del software.

Las especificaciones del software deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.

El software que se desarrolle deberá incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.

Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.

Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.

Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.

El acceso al código fuente de los aplicativos deberá estar limitado a las personas del servicio.

En el entorno de pruebas sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.

Durante las pruebas de los aplicativos se verificará que no existen brechas de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.

Sólo se transferirá al entorno de producción aquel software que haya sido expresamente aprobado.

En relación con los servicios Web se considerará la gestión del Top 10 de Owasp (https://owasp.org/www-project-top-ten/)

4.15. Gestión de contingencias

El servicio deberá contar con un plan que permite su prestación aun en caso de contingencias.

El plan anterior deberá ser desarrollado en función de los eventos capaces de causar interrupciones en el servicio y su probabilidad de ocurrencia.

La organización proveedora deberá poder demostrar la viabilidad del plan de contingencias existente.

5. Seguimiento y control

Con el fin de velar por el correcto uso de los mencionados recursos, a través de los mecanismos formales y técnicos que se considere oportunos, la Organización comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente.

MIKEL CEARSOLO CABREJAS CEO LUDUS TECH S.L.

Ludus Tech, S.L.
C.I.F. B-95661856
ludusglobal.com
+34 946 12 22 41