Augustus Capital AM

MANUAL DE PROTOCOLOS DE SEGURIDAD DE LA INFORMACIÓN DE AUGUSTUS CAPITAL ASSET MANAGEMENT, S.G.I.I.C., S.A.

SEPTIEMBRE 2024

FECHA	CAMBIOS	REDACIÓN	VERSIÓN
Abril 2020	Cumplimiento Normativo	1ª redacción	1.0
Septiembre 2024	Cumplimiento Normativo	2ª redacción	2.0

1. INTRODUCCIÓN

El objetivo del presente manual es describir los procedimientos de seguridad de la información de Augustus Capital S.G.I.I.C., S.A. (en adelante, "Augustus Capital" o la "Entidad").

En este sentido cabe destacar que las previsiones contenidas en este manual tienen como fin el aumento de la seguridad de la información de Augustus Capital contenida en el dispositivo.

1.1. Área responsable de la elaboración del procedimiento

La responsabilidad de la elaboración y actualización de este procedimiento recae en la Unidad de Cumplimiento Normativo, con la colaboración del resto de áreas de actividad de la Organización que se vean implicadas.

1.2. Órganos responsables de la aprobación del procedimiento

El Consejo de Administración es el responsable de la aprobación de las modificaciones de este procedimiento.

Será responsabilidad del Consejo de Administración fijar la estrategia empresarial de la Entidad y sus distintas áreas de negocio y garantizar que la organización cuente con medios humanos y materiales que procuren tanto la adecuada gestión del negocio como una suficiente segregación de funciones y control de los riesgos asumidos. Así, el Consejo de Administración dictará las políticas específicas que regirán la actividad de la Entidad y definirá los criterios para la elaboración y revisión de los procedimientos.

En el proceso de actualización del procedimiento se tendrá en consideración todas las modificaciones que consideren necesarias como consecuencia de:

- Los informes que le son remitidos al Consejo de Administración
- Las propuestas del resto de la Organización
- Las incidencias detectadas en los sistemas de control y
- Las recomendaciones de los auditores externos y organismos supervisores.

En cualquier caso, la revisión de los procedimientos internos será permanente y la Unidad de Cumplimiento Normativo podrá trasladar al Consejo de Administración, en cualquier momento, cuantas propuestas de mejora considere oportuno realizar, y ello a iniciativa propia o del responsable de cualquier otra área de la Entidad.

1.3. Destinatarios del procedimiento

Una vez aprobado por el Consejo de Administración, este documento, y sus sucesivas versiones y actualizaciones o modificaciones, será circularizado entre los sujetos destinatarios. Los sujetos destinatarios del presente documento son todos los empleados y directivos y constando una copia de la última versión actualizada del mismo

en los servidores de la Entidad a disposición de los mencionados sujetos. No obstante, los miembros del Departamento de Administración son los destinatarios más directos de este procedimiento.

Los directores de los departamentos estarán permanentemente informados de las incidencias que se produzcan en relación con su cumplimiento y las trasladarán a los empleados de sus departamentos, al objeto de que se adopten las medidas necesarias para corregirlas y se propongan, en su caso, modificaciones en los procedimientos implantados.

En todo caso, comunicarán al responsable de la función de Cumplimiento Normativo las situaciones graves que se hubieran producido antes de tomar cualquier medida para subsanarlas.

2. PROTOCOLOS DE SEGURIDAD DE LA INFORMACIÓN

2.1 Definición

Este manual es de aplicación tanto a dispositivos ubicados en la oficina como a los dispositivos móviles.
-"Dispositivos ubicados en la oficina": todos aquellos ordenadores de sobremesa, portátiles, tablet, etc. propiedad de Augustus Capital radicadas en la oficina de trabajo.
-"Dispositivos móviles" todos aquellos aparatos tecnológicos que no están físicamente ubicados en las oficinas de Augustus Capital Asset Management. Por lo tanto, serán considerados dispositivos móviles los ordenadores portátiles o de sobremesa, las tablets, teléfonos móviles, etc. utilizados por los trabajadores de Augustus Capital para el desempeño de su trabajo, siendo estos los de la empresa.

2.2 Seguridad en ordenadores

Se tendrán en cuenta las siguientes recomendaciones:

-Los ordenadores deberán contar siempre con un antivirus activado. Es posible utilizar el antivirus que por defecto se proporciona en Windows 10, el "Windows Defender".

-Es recomendable contar con contraseña de firmware o de BIOS / UEFI, especialmente importante en el caso de ordenadores portátiles. Para establecer la contraseña de BIOS/UEFI se puede ver un tutorial en la siguiente página: *https://www.solvetic.com/tutoriales/article/2843-como-establecer-contrasena-en-bios-o-uefi-en-windows-10/*

-Los usuarios deben contar siempre con una cuenta de usuario, y esa cuenta de usuario debe ser lo suficientemente robusta (mayúsculas, minúsculas, números, símbolos, etc. cuanto más larga y compleja, mejor) y modificarse de forma periódica.

-Cuando no se use el dispositivo debe bloquearse (combinación de teclas Windows+L).

-Tratamiento de la información confidencial. La información corporativa que no sea estrictamente necesaria para el desarrollo de las tareas del usuario no deberá almacenarse en el dispositivo. Para ello, se recomienda trabajar directamente en la nube, sin descargar los ficheros en el dispositivo personal. Si el dispositivo también es de uso personal, se deberá borrar toda la información confidencial de la empresa que contenga cuando el contrato entre ambas partes se haya extinguido.

-En el caso excepcionar de descargar información sensible en el dispositivo personal se utilizará el aplicativo "aescrypt" para encriptar la información (https://www.aescrypt.com/).

-Precaución al abrir correos de destinatarios no conocidos, sobre todo si solicitan claves (phishing) o contienen archivos ejecutables (.exe).

-No se instalarán nuevos programas sin la supervisión/conformidad de la Unidad de Cumplimiento Normativo.

-Se deberá guardar todas las precauciones posibles con la información de clientes archivadas tanto en la carpeta compartida como en formato físico.

-Cuidado al enviar correos electrónicos con información sensible tanto de Augustus Capital como de los clientes.

-No deben conectarse a redes Wi-Fi públicas. Si necesitamos conectarnos es preferible la utilización de los datos del teléfono móvil.

-Es conveniente la utilización de VPN. Los VPN son "túneles" de información que evita que nuestra información pueda ser espiada por terceros.

Para la creación de una VPN visitar la página web https://protonvpn.com/ >> "get protonvpn free" >> creamos una cuenta de usuario >> bajamos el cliente para Windows 10 y nos conectamos.
Los servidores gratuitos están en Países Bajos, EE.UU. y Japón. Para el periodo de prueba podemos utilizar cualquier servidor del mundo, aunque SIEMPRE utilizar servidores en la UE. Una vez pasado el periodo de prueba utilizaremos siempre los servidores FREE de Países Bajos.

La utilización de VPN puede hacer que la conexión sea más lenta de lo habitual.

2.3 Seguridad en teléfonos móviles

Se tendrán en cuenta las siguientes recomendaciones:

-Los teléfonos móviles deberán contar con sistemas de bloqueo con un plazo de aplicación lo menor posible. Serán permitidos tanto sistemas de desbloqueo por PIN como por huella dactilar o escáner visual.

-En el caso de utilización de PIN, la contraseña debe ser lo suficientemente robusta para no ser detectada fácilmente. Bajo ningún concepto debe llevarse apuntado el PIN en el teléfono móvil.

-No deben conectarse a redes Wi-Fi públicas.

-En el caso excepcionar de almacenar información de Augustus Capital en el teléfono móvil (fuera del OneDrive) deberá hacer una copia de seguridad periódica.

-Precaución al abrir correos de destinatarios no conocidos, sobre todo si solicitan claves (phishing) o contienen archivos ejecutables (.exe).

-Precaución al instalar apps que puedan comprometer la seguridad de la información y los datos tanto privados como de Augustus Capital.

-Utilización de software original.

-Instalación de software que permite rastrear el dispositivo en caso de robo o pérdida del dispositivo.

-Apagar el *bluetooth* si no se está utilizando (consume batería y es fuente de entrada al teléfono).

-Solicitar confirmación cada vez que un dispositivo *bluetooth* está intentando conectar con el equipo.

-Configurar el *bluetooth* para que no se publique la información de la identidad al entorno (modo invisible).

-Nunca conectarse a otro dispositivo *bluetooth* que no conozcamos.

-Evitar emparejamientos por *bluetooth* en lugares públicos.

2.4 Pasos a seguir en caso de entrada de virus

En el caso de que se haya producido la infección del dispositivo, realizar los siguientes procedimientos:

a) Comunicación urgente a la Unidad de Cumplimiento y a la Dirección para aislar el virus y que no se propague a la red interna, en la medida de lo posible.

b) Escanear el PC con el antivirus instalado y eliminar los virus existentes.

c) Si el antivirus habitual no los detecta, escanear el PC con un antivirus "en línea" (necesitas tener Internet Explorer con ActiveX autorizado). Se recomienda el siguiente enlace: https://www.pandasecurity.com/es/homeusers/solutions/online-antivirus/?ref=activescan
Anotar el nombre del virus y de los archivos infectados, pero no selecciones la opción eliminar el virus ya que algunas infecciones infectan los archivos de Windows y si los eliminas puede plantarse el sistema.

d) Actualización manual o forzada del antivirus instalado en el dispositivo.

e) Actualización del sistema operativo.

f) Del mismo modo, en el supuesto de que esa entrada de virus afecte a la seguridad de los datos de carácter personal, la Unidad de Cumplimiento, comunicará dichos hechos (dentro de las primeras 24 horas) al Delegado de Protección de Datos. El Delegado de Protección (en colaboración con la Unidad de Cumplimiento) analizará la posible brecha de seguridad (conforme a lo establecido en la IT-RGPD/LOPDGDD "Brechas de Seguridad"), y comunicará a la Unidad de Cumplimiento y a la Dirección las medidas a adoptar (notificación a la Autoridad de Control, a los propios interesados, etc.).

En el caso de que no se pueda solucionar el virus detectado se procederá a formatear el dispositivo y cargar de nuevo la información.

2.5 Pasos a seguir en caso de pérdida o robo del dispositivo.

En el caso de que se haya producido la pérdida o robo del dispositivo, realizar los siguientes procedimientos:

-Del mismo modo, en el supuesto de que la pérdida o robo de dispositivos, afecte a la seguridad de los datos de carácter personal, la Unidad de Cumplimiento, comunicará dichos hechos (dentro de las primeras 24 horas) al Delegado de Protección de Datos. El Delegado de Protección (en colaboración con la Unidad de Cumplimiento) analizará la posible brecha de seguridad (conforme a lo establecido en la IT-RGPD/LOPDGDD "Brechas de Seguridad"), y comunicará a la Unidad de Cumplimiento y a la Dirección las medidas a adoptar (notificación a la Autoridad de Control, a los propios interesados, etc.).

-Rastrear el dispositivo con la aplicación de rastreo activada, en el caso de estar activado.

-Urgentemente denunciar ante la Policía Nacional.

-Llamar al operador telefónico para bloquear la tarjeta SIM del dispositivo (se debe aportar la denuncia).

-En el caso de disponer de borrado en remoto de la información, solicitar el borrado de la información del dispositivo.